Journal of Number Theory **82**, 188–224 (2000)
doi:10.1006/jnth.1999.2414, available online at http://www.idealibrary.com on IDEAL®

Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern

K. Wildanger

Fachbereich 3 Mathematik, MA 8-1, Technische Universität Berlin, Straße des 17. Juni 136, 10623 Berlin, Germany

Communicated by M. Pohst

Received December 23, 1998

Let $\mathcal{K}$ be an algebraic number field with non-zero $\alpha, \beta \in \mathcal{K}$. Siegel showed in 1929 that there are only finitely many units $\varepsilon_1, \varepsilon_2$ in K which satisfy the unit equa-

equations in number fields up to unit rank 10 and with more than 100,000 solutions are solved. By applying our algorithm to index form equations we compute all power integral bases in the cyclotomic number fields up to degree 12 and in $\mathbb{Q}(\zeta_{17})$, $\mathbb{Q}(\zeta_{19})$, $\mathbb{Q}(\zeta_{23})$. © 2000 Academic Press

In dieser Arbeit wird das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern behandelt. Beiden Problemstellungen ist gemein, daß sie jeweils nur endlich viele Lösungen besitzen. Algorithmen zur vollständigen Berechnung dieser Lösungen wurden möglich durch Ergebnisse von A. Baker zu Linearformen in den Logarithmen algebraischer Zahlen.

Das Lösen einer Einheitengleichung besteht im wesentlichen aus drei Schritten. Zuerst leitet man anhand der Resultate Bakers große obere Schranken für die Lösungen her. Diese Schranken werden im zweiten Schritt des Verfahrens mit dem LLL-Algorithmus reduziert. Im letzten Schritt, welcher die weitaus meiste Rechenzeit beansprucht, müssen all unterhalb der Schranken liegenden Einheiten daraufhin überprüft werden, ob sie Lösungen der Einheitengleichung sind. Wir beschrieben im ersten Abschnitt dieser Arbeit ein neues Verfahren, mit dem diese Überprüfung effizienter als bislang durchgeführt werden kann. Mit dem Verfahren, welches Methoden aus der Geometrie der Zahlen benutzt, lösten wir Einheitengleichungen in Zahlkörpern bis hin zum Einheitenrang 10. Als Beispiel behandeln wir hier das Lösen einer Einheitengleichung in $\mathbb{Q}(\zeta_{19})$.

Im zweiten Abschnitt setzen wir dann Einheitengleichungen zum Lösen von Indexformgleichungen ein. Erstmals konnten Indexformgleichungen in Zahlkörpern vom Grad 8, 10, 12, 16, 18 und 22 gelöst werden. Für die

0022-314X/00 $35.00

Implementierung unserer Verfahren wurde das Computeralgebra-System KANT [3] verwendet. Alle Beispiele wurden auf einer SGI Origin 2000 gerechnet.

Wir fixieren einige Schreibweisen, die während der gesamten Arbeit beibehalten werden. $\mathscr{K}$ bezeichne stets einen algebraischen Zahlkörper vom Grad $n>1$ über $\mathbb{Q}$. Es sei jeweils $\mathscr{K}=\mathbb{Q}(\theta)$, wobei $\theta\in\mathbb{C}$ Nullstelle eines normierten und irreduziblen Polynoms mit ganzzahligen Koeffizienten sei, welches r_1 reelle und $2r_2$ komplexe Nullstellen habe. Die n verschiedenen $\mathbb{Q}$-Einbettungen (Konjugationen) von $\mathscr{K}$ in $\mathbb{C}$ seien gegeben durch $\sigma_1, ..., \sigma_n$. Ist $j\in\{1, ..., n\}$, so schreiben wir $\alpha^{(j)}=\sigma_j(\alpha)$ für die j-te Konjugierte einer algebraischen Zahl $\alpha\in\mathscr{K}$. Die Konjugationen seien in gewohnter Weise numeriert:

(i) $\theta^{(1)}, ..., \theta^{(r_1)}\in\mathbb{R}$,

(ii) $\theta^{(r_1+1)}, ..., \theta^{(r_1+r_2)}\in\mathbb{C}\setminus\mathbb{R}$,

(iii) $\theta^{(r_1+r_2+j)}=\overline{\theta^{(r_1+j)}} (1\leqslant j\leqslant r_2)$.

Wir setzen $\mathscr{I}:=\{1, ..., r_1+r_2\}$.

Den ganzen Abschluß von $\mathbb{Z}$ in $\mathscr{K}$ bezeichnen wir mit $\mathfrak{o}_{\mathscr{K}}$. Es sei $\mathrm{U}_{\mathscr{K}}$ die Einheitengruppe von $\mathfrak{o}_{\mathscr{K}}$, und $\mathrm{TU}_{\mathscr{K}}$ sei die endliche zyklische Gruppe der in $\mathfrak{o}_{\mathscr{K}}$ gelegenen Einheitswurzeln. Ist $\mathscr{L}$ ein weiterer algebraischer Zahlkörper, so verwenden wir analog die Bezeichnungen $\mathfrak{o}_{\mathscr{L}}$, $\mathrm{U}_{\mathscr{L}}$ und $\mathrm{TU}_{\mathscr{L}}$. Ein unitärer Teilring R von $\mathfrak{o}_{\mathscr{K}}$ heißt Ordnung von $\mathscr{K}$, falls R ein freier $\mathbb{Z}$-Modul vom Rang n ist. Für die Diskriminante einer Ordnung R von $\mathscr{K}$ schreiben wir $\mathrm{disc}\, R$ und speziell $\mathrm{disc}_{\mathscr{K}}$ für die Diskriminante der Maximalordnung $\mathfrak{o}_{\mathscr{K}}$. Die Diskriminante eines Polynoms $f(t)\in\mathbb{Z}[t]$ notieren wir als $\mathrm{disc}\, f$.

1. EINHEITENGLEICHUNGEN

Als eine Einheitengleichung bezeichnet man eine Gleichung der Gestalt

$$\alpha a+\beta b=1, \tag{1.1}$$

deren Koeffizienten α, β Elemente eines algebraischen Zahlkörpers $\mathscr{K}$ mit $\alpha\beta\neq 0$ sind und deren Unbekannten a, b Einheiten aus $\mathrm{U}_{\mathscr{K}}$ sind. Unter dem Lösen einer solchen Einheitengleichung ist die Bestimmung aller der nach einem Satz von Siegel [22] endlich vielen Paare $(a, b)\in\mathrm{U}_{\mathscr{K}}\times\mathrm{U}_{\mathscr{K}}$ zu verstehen, welche der Gleichung (1.1) genügen.

Einheitengleichungen sind ein nützliches Werkzeug beim Lösen diophantischer Gleichungen. So lassen sich das Lösen von Indexform- und Thue-Gleichungen sowie die Berechnung der ganzen Punkte auf superelliptischen Kurven auf das Lösen von Einheitengleichungen zurückführen [13, 25].

Einschränkend muß hierzu allerdings gesagt werden, daß bei solchen Problemtransformationen die algebraischen Zahlkörper, welche den zu lösenden Einheitengleichungen dann zugrunde liegen, oftmals so hohen Grad besitzen, daß in der Praxis eben diese Einheitengleichungen nicht gelöst werden können.

Sei nun für den Rest des Abschnitts $\mathscr{K}$ ein beliebiger, aber fest gewählter algebraischer Zahlkörper. Es bezeichne $r := r_1 + r_2 - 1$ den Einheitenrang von $\mathscr{K}$ und $w \in 2\mathbb{Z}$ die Anzahl der Elemente von $\mathrm{TU}_{\mathscr{K}}$. Ferner seien $\zeta \in \mathrm{U}_{\mathscr{K}}$ ein fest gewählter Erzeuger von $\mathrm{TU}_{\mathscr{K}}$ und $\varepsilon_1, ..., \varepsilon_r$ ein fest gewähltes Grundeinheitensystem von $\mathrm{U}_{\mathscr{K}}$.

Beliebig, aber gleichfalls fest gewählt für den Rest des Abschnitts seien $\alpha, \beta \in \mathscr{K}^{\times}$. Die Lösungsmenge der Einheitengleichung aus (1.1) ist dann gegeben durch

$$\mathfrak{L} := \{(a, b) \in \mathrm{U}_{\mathscr{K}} \times \mathrm{U}_{\mathscr{K}} \mid \alpha a + \beta b = 1\}.$$

Für Einheitenrang $r = 0$, also $\mathrm{TU}_{\mathscr{K}} = \mathrm{U}_{\mathscr{K}}$, ist die Bestimmung von $\mathfrak{L}$ trivial, für $r = 1$ kann $\mathfrak{L}$ leicht anhand einer elementaren Abschätzung berechnet werden [27]. Ist der Einheitenrang r—wie im folgenden stets vorausgesetzt—größer als 1, so ist das Lösen der Einheitengleichung (1.1) weitaus schwieriger. Die explizite Bestimmung von $\mathfrak{L}$ ist in diesem Fall erst durch die sogenannte Bakersche Methode möglich geworden, welche auch Grundlage für das im folgenden vorgestellte Verfahren ist. Bevor wir mit dessen Darstellung beginnen, fixieren wir einige Notationen:

Ist $\varepsilon = \xi \varepsilon_1^{e_1} \cdots \varepsilon_r^{e_r} \in \mathrm{U}_{\mathscr{K}}$ ($\xi \in \mathrm{TU}_{\mathscr{K}}$, $e_1, ..., e_r \in \mathbb{Z}$), so definieren wir $\bar{\varepsilon} \in \mathbb{Z}^{\geqslant 0}$ durch

$$\bar{\varepsilon} := \max_{1 \leqslant i \leqslant r} |e_i|.$$

Weiter setzen wir

$$\mathfrak{L}_{\alpha} := \{a \in \mathrm{U}_{\mathscr{K}} \mid \exists b \in \mathrm{U}_{\mathscr{K}} : (a, b) \in \mathfrak{L} \wedge \bar{a} \leqslant \bar{b}\}, \tag{1.2}$$

$$\mathfrak{L}_{\beta} := \{b \in \mathrm{U}_{\mathscr{K}} \mid \exists a \in \mathrm{U}_{\mathscr{K}} : (a, b) \in \mathfrak{L} \wedge \bar{b} \leqslant \bar{a}\}. \tag{1.3}$$

Es gilt offensichtlich

$$\mathfrak{L} = \{(a, b) \in \mathfrak{L} \mid a \in \mathfrak{L}_{\alpha}\} \cup \{(a, b) \in \mathfrak{L} \mid b \in \mathfrak{L}_{\beta}\}.$$

Mit Log bezeichnen wir fortan den Hauptzweig des komplexen Logarithmus, also $\mathrm{Log}\, z = \log |z| + i \,\mathrm{Arg}\, z \;\forall z \in \mathbb{C}^{\times}$, wobei das Argument durch die Bedingung $\mathrm{Arg}(\mathbb{C}^{\times}) = (-\pi, \pi]$ normiert sei. Zu $x \in \mathbb{R}$ bezeichne $\lfloor x \rceil \in \mathbb{Z}$ die nächstgelegene ganze Zahl, für $z \in \mathbb{C}$ se $\Re z$ der Real- und $\Im z$ der Imaginärteil von z.

1.1. *Die Bakersche Methode*

Wir bestimmen eine obere Schranke $A = A(\mathscr{K}, \alpha, \beta) \in \mathbb{Z}^{\geqslant 0}$ mit

$$\bar{a} \leqslant A \qquad \forall a \in \mathfrak{Q}_\alpha. \tag{1.4}$$

Analog kann $B \in \mathbb{Z} \geqslant 0$ berechnet werden, so daß $\bar{b} \leqslant B \ \forall b \in \mathfrak{Q}_\beta$.

Die Schreibweise $A = A(\mathscr{K}, \alpha, \beta)$ soll verdeutlichen, daß A von $\mathscr{K}$ sowie von α und β abhängt, wobei für $\mathscr{K}$ ein fest gewähltes Grundeinheitensystem vorausgesetz ist.

LEMMA 1.1. *Es existiert* $c_1 = c_1(\mathscr{K}) > 0$, *so daß es zu jedem* $\varepsilon \in \mathrm{U}_\mathscr{K}$ *mindestens ein* $\mu = \mu(\varepsilon) \in \mathscr{I}$ *gibt mit*

$$\log |\varepsilon^{(\mu)}| \leqslant -c_1 \bar{\varepsilon}. \tag{1.5}$$

Beweis. Sei $\varepsilon = \xi \varepsilon_1^{e_1} \cdots \varepsilon_r^{e_r} \in \mathrm{U}_\mathscr{K}$ $(\xi \in \mathrm{TU}_\mathscr{K},\ e_1, ..., e_r \mathbb{Z})$ beliebig. Wähle $J \in \{1, ..., r\}$ so daß

$$|\log |\varepsilon^{(J)}|| = \max_{1 \leqslant j \leqslant r} |\log |\varepsilon^{(j)}||.$$

Mit $L := (\log |\varepsilon_k^{(i)}|)_{1 \leqslant i, k \leqslant r}$, $e := (e_k)_{1 \leqslant k \leqslant r}$ gilt $L \cdot e = (\log |\varepsilon^{(i)}|)_{1 \leqslant i \leqslant r}$, und ist $c > 0$ die Zeilensummennorm von L^{-1}, so folgt

$$\bar{\varepsilon} \leqslant c\, |\log |\varepsilon^{(J)}||. \tag{1.6}$$

Setze $c_1 := 1/(n-1)\, c$. Angenommen, es gilt $\log |\varepsilon^{(j)}| > -c_1 \bar{\varepsilon}\ \forall j \in \mathscr{I}$. Aus (1.6) erhalten wir wegen $\varepsilon \in \mathrm{U}_\mathscr{K}$ dann

$$|\log |\varepsilon^{(J)}|| \geqslant \frac{\bar{\varepsilon}}{c} = (n-1)\, c_1 \bar{\varepsilon} > -\sum_{\substack{j=1 \\ j \neq J}}^{n} \log |\varepsilon^{(j)}| = \log |\varepsilon^{(J)}|,$$

also $\log |\varepsilon^{(J)}| < 0$. Nach (1.6) ist somit

$$-\bar{\varepsilon} \geqslant c \log |\varepsilon^{(J)}| \geqslant \frac{1}{c_1} \log |\varepsilon^{(J)}|,$$

was im Widerspruch zur Annahme steht. ∎

Bemerkung 1.2. Für total komplexe $\mathscr{K}$ ist schärfer $c_1 := 1/(n/2-1)\, c$ im Beweis zu 1.1. möglich.

LEMMA 1.3. *Sei* $a \in \mathfrak{Q}_\alpha$ *beliebig. Dann existieren* $\mu = \mu(a) \in \mathscr{I}$ *und* $c_{2,\mu} = c_2(\mathscr{K}, \beta, \mu) > 0$ *mit*

$$|(\alpha a)^{(\mu)} - 1| \leqslant c_{2,\mu} \exp(-c_1 \bar{a}). \tag{1.7}$$

Beweis. Sei $b \in \mathrm{U}_{\mathscr{K}}$ mit $\alpha a + \beta b = 1$. Nach 1.1 existiert ein $\mu \in \mathscr{I}$ mit $\log |b^{(\mu)}| \leqslant -c_1 \bar{b}$. Setzen wir $c_{2,\mu} := |\beta^{(\mu)}|$, so folgt wegen $\bar{a} \leqslant \bar{b}$ sogleich

$$|(\alpha a)^{(\mu)} - 1| = |(\beta b)^{(\mu)}| \leqslant c_{2,\mu} \exp(-c_1 \bar{a}). \quad \blacksquare$$

Definieren wir für jedes $\mu \in \mathscr{I}$ die Menge $\mathfrak{L}_{\alpha,\mu} \subseteq \mathfrak{L}_\alpha$ durch

$$\mathfrak{L}_{\alpha,\mu} := \{a \in \mathfrak{L}_\alpha \mid |(\alpha a)^{(\mu)} - 1| \leqslant c_{2,\mu} \exp(-c_1 \bar{a})\},$$

so folgt aus 1.3 unmittelbar

$$\mathfrak{L}_\alpha = \mathfrak{L}_{\alpha,1} \cup \cdots \cup \mathfrak{L}_{\alpha, r_1 + r_2}. \tag{1.8}$$

Sei nun im weiteren $\mu \in \mathscr{I}$ beliebig, aber fest vorgegeben. Ohne Einschränkung sei der Erzeuger ζ von $\mathrm{TU}_{\mathscr{K}}$ so gewählt, daß $2\pi i = w \operatorname{Log} \zeta^{(\mu)}$. Wir werden ein Resultat von Baker zu Linearformen in den Logarithmen algebraischer Zahlen einsetzen, um eine obere Schranke $A_{2,\mu}$ herzuleiten, so daß

$$\bar{a} \leqslant A_{2,\mu} \qquad \forall a \in \mathfrak{L}_{\alpha,\mu}. \tag{1.9}$$

Für unsere Zwecke reicht es, wenn wir uns auf homogene Linearformen in den Logarithmen algebraischer Zahlen beschränken, deren Koeffizienten ganzzahlig sind. Eine solche Linearform ist ein Ausdruck

$$\Lambda = g_1 \operatorname{Log} \gamma_1 + \cdots + g_k \operatorname{Log} \gamma_k$$

mit algebraischen Zahlen $\gamma_i \neq 0$ $(1 \leqslant i \leqslant k)$ und $g_1, \ldots, g_k \in \mathbb{Z}$. Wir setzen $G := \max_{1 \leqslant i \leqslant k} |g_i|$. Eines der Resultate Bakers besteht darin, eine nur von $\gamma_1, \ldots, \gamma_k$ abhängige, effektiv berechenbare Konstante $C > 0$ anzugeben, so daß unter der Voraussetzung $\Lambda \neq 0$ die Abschätzung

$$0 < G^{-C} \leqslant |\Lambda| \tag{1.10}$$

erfüllt ist. Der ursprünglich von Baker angegebene Wert für die Konstante C in (1.10) wurde mehrfach verbessert. Für unsere Rechnungen verwendeten wir ein Ergebnis von Baker und Wüstholz [1] aus dem Jahre 1993, dessen Formulierung hier an die obige Situation angepaßt ist.

Satz 1.4 (Baker/Wüstholz). *Seien $g_1, \ldots, g_k$, $\gamma_1, \ldots, \gamma_k$ und G wie oben gegeben. Es sei $h(\gamma_i)$ die absolute logarithmische Höhe von γ_i $(1 \leqslant i \leqslant k)$, also*

$$h(\gamma_i) = \frac{1}{d_i} \log \left(a_{i,0} \prod_{j=1}^{d_i} \max(1, |\gamma_i^{(j)}|) \right),$$

wobei $a_{i,0}t^{d_i} + a_{i,1}t^{d_i-1} + \cdots + a_{i,d_i} \in \mathbb{Z}[t]$, $a_{i,0} > 0$, $\operatorname{ggT}(a_{i,0}, ..., a_{i,d_i}) = 1$, *das Minimalpolynom von* γ_i *sei. Ferner seien* $d \in \mathbb{N}$ *und* $h_i > 0$ $(1 \leqslant i \leqslant k)$ *definiert über*

$$d := [\mathbb{Q}(\gamma_1, ..., \gamma_k): \mathbb{Q}],$$

$$h_i := \max\left(h(\gamma_i), \frac{|\operatorname{Log}\gamma_i|}{d}, \frac{1}{d}\right).$$

Gelten dann $\Lambda \neq 0$ *and* $G \geqslant 3$, *so kann* C *in* (1.10) *gewählt werden als*

$$C = 18(k+1)!\, k^{k+1} 32^{k+2} d^{k+1} \log(2kd)\, h_1 \cdots h_k.$$

Wir fixieren ein beliebiges

$$a = \zeta^{a_0}\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} \in \mathfrak{Q}_\alpha \qquad \left(a_0 \in \left\{-\frac{w}{2}+1, ..., \frac{w}{2}\right\}, a_1, ..., a_r \in \mathbb{Z}\right). \tag{1.11}$$

Es sei $b \in \mathrm{U}_{\mathscr{K}}$ mit $(a, b) \in \mathfrak{Q}$. Um (1.10) zur Bestimmung der oberen Schranke $A_{2,\mu}$ einzusetzen, benötigen wir zunächst eine geeignete Linearform in den Logarithmen algebraischer Zahlen. Eine solche erhalten wir aus

$$\Lambda_\mu := \operatorname{Log}(\alpha a)^{(\mu)} \neq 0 \tag{1.12}$$

durch Anwendung der Funktionalgleichung

$$\operatorname{Log}(z_1 \cdots z_m) = \operatorname{Log} z_1 + \cdots + \operatorname{Log} z_m + k(z_1, ..., z_m)\,\pi i \qquad \forall z_1, ..., z_m \in \mathbb{C}^\times,$$

wobei $k(z_1, ..., z_m) \in 2\mathbb{Z}$ mit $|k(z_1, ..., z_m)| \leqslant m$.

Aufgrund von $a_0 \in \{-(w/2)+1, ..., (w/2)\}$ existiert $a_{r+1} = a_{r+1}(\mathscr{K}, \alpha, \mu, a) \in 2\mathbb{Z}$ mit $|a_{r+1}| \leqslant 1 + (w/2) + r\bar{a}$, so daß

$$\Lambda_\mu = \operatorname{Log}\alpha^{(\mu)} + a_0 \operatorname{Log}\zeta^{(\mu)} + \sum_{i=1}^{r} a_i \operatorname{Log}\varepsilon_i^{(\mu)} + a_{r+1}\, i\pi.$$

Indem wir $a_0' := a_0 + (w/2)\, a_{r+1}$ setzen, können wir die Terme $a_0 \operatorname{Log}\zeta^{(\mu)}$ und $a_{r+1} i\pi$ zusammenfassen, also

$$\Lambda_\mu = \operatorname{Log}\alpha^{(\mu)} + a_0' \frac{2\pi i}{w} + \sum_{i=1}^{r} a_i \operatorname{Log}\varepsilon_i^{(\mu)}.$$

Wir setzen

$$\bar{\bar{a}} := \max(|a_0'|, \bar{a}) \qquad \text{und} \qquad A_{1,\mu} := \max\left(3, \frac{\log(2c_{2,\mu})}{c_1}\right). \tag{1.13}$$

LEMMA 1.5. *Es existieren* $c_3 = c_3(\mathcal{K})$, $c_{4,\mu} = c_4(\mathcal{K}, \beta, \mu) > 0$, *so daß unter der Voraussetzung* $\bar{a} \geqslant A_{1,\mu}$ *gilt*:

$$|\Lambda_\mu| \leqslant \tfrac{3}{2} c_{2,\mu} \exp(-c_1 \bar{a}) \leqslant c_{4,\mu} \exp(-c_3 \bar{\bar{a}}). \tag{1.14}$$

Beweis. Mittels Lemma 1.3 folgt aus $\bar{a} \geqslant A_{1,\mu}$ zunächst

$$|(\alpha a)^{(\mu)} - 1| \leqslant \tfrac{1}{2}. \tag{1.15}$$

Beachten wir

$$\begin{aligned} |\mathrm{Log}(1+z)| &\leqslant |z| + \frac{1}{2} \sum_{k=2}^{\infty} |z|^k \\ &= |z| + \frac{1}{2} \frac{|z|^2}{1-|z|} \leqslant \frac{3}{2} |z| \qquad \forall z \in \mathbb{C}, \quad |z| \leqslant \frac{1}{2}, \end{aligned}$$

so erhalten wir aus (1.15) und 1.3 mit

$$\begin{aligned} |\Lambda_\mu| &= |\mathrm{Log}(1 + ((\alpha a)^{(\mu)} - 1))| \\ &\leqslant \tfrac{3}{2} |(\alpha a)^{(\mu)} - 1| \leqslant \tfrac{3}{2} c_{2,\mu} \exp(-c_1 \bar{a}) \end{aligned} \tag{1.}$$

die linke Ungleichung in (1.14). Es ist $\bar{\bar{a}} \leqslant w/2(2 + (w/2) + r\bar{a})$, also

$$-\bar{a} \leqslant \frac{1}{r}\left(2 + \frac{w}{2}\right) - \frac{2}{rw}\,\bar{\bar{a}}.$$

Hieraus ergibt sich die rechte Ungleichung in (1.14), indem c_3 und $c_{4,\mu}$ definiert werden als

$$c_3 := c_1 \frac{2}{rw}, \qquad c_{4,\mu} := \frac{3}{2} c_{2,\mu} \exp\left(\frac{c_1}{r}\left(2 + \frac{w}{2}\right)\right). \quad \blacksquare$$

Aus der Gegenüberstellung der unteren Schranke für $|\Lambda_\mu|$ aus (1.10) und der oberen Schranke in (1.14) erhalten wir unter der Voraussetzung $\bar{a} \geqslant A_{1,\mu}$ die Abschätzung

$$\bar{\bar{a}}^{-C} \leqslant |\Lambda_\mu| \leqslant c_{4,\mu} \exp(-c_3 \bar{\bar{a}}), \tag{1.17}$$

womit implizit eine obere Schranke $A_{3,\mu}$ für $\bar{\bar{a}}$ gegeben ist. $A_{2,\mu} := \max(A_{1,\mu}, A_{3,\mu})$ erfüllt dann (1.9), und aufgrund von (1.8) kann A in (1.4) als

$$A := \max_{1 \leqslant \mu \leqslant r_1 + r_2} \lfloor A_{2,\mu} \rfloor \tag{1.18}$$

gewählt werden.

Wiewohl mit der Bestimmung von oberen Schranken für die Exponenten im Prinzip alle Lösungen der Einheitengleichung (1.1) durch einfaches Ausprobieren berechnet werden können, so sind doch diese Schranken viel zu groß, um ein solches Ausprobieren in vertretbarer Zeit durchzuführen. Dies mag das folgende, später fortgesetzte Beispiel illustrieren, dem wir eine Bemerkung voranstellen.

Bemerkung 1.6. Ist $\mu \in \{1, ..., r_1\}$, so können wir zur Herleitung der oberen Schranke $A_{2,\mu}$ alternativ die reelle Linearform

$$\Lambda'_\mu = \log |(\alpha a)^{(\mu)}| = \log |\alpha^{(\mu)}| + \sum_{i=1}^{r} a_i \log |\varepsilon_i^{(\mu)}| \tag{1.19}$$

verwenden. Unter den Voraussetzungen $\bar{a} \geqslant A_{1,\mu}$ und $\alpha a \neq -1$ erhält man analog zum Beweis von 1.5 in Verbindung mit (1.10) die Abschätzung

$$\bar{a}^{-C} \leqslant |\Lambda'_\mu| \leqslant \tfrac{3}{2} c_{2,\mu} \exp(-c_1 \bar{a}). \tag{1.20}$$

Beispiel 1.7. Für die primitive 19-te Einheitswurzel $\zeta_{19} = \exp(2\pi i/19)$ setzen wir $\theta := \zeta_{19} + \zeta_{19}^{-1}$. Dann ist $\mathscr{K} = \mathbb{Q}(\theta)$ der maximale reelle Teilkörper von $\mathbb{Q}(\zeta_{19})$ mit $[\mathscr{K} : \mathbb{Q}] = 9$, $r = 8$ und $\mathfrak{o}_\mathscr{K} = \mathbb{Z}[\theta]$. Die Konjugierten von θ seien numeriert als $\theta^{(k)} = 2\cos(2\pi k/19)$ $(1 \leqslant k \leqslant 9)$, und ein Grundeinheitensystem in $\mathfrak{o}_\mathscr{K}$ sei gegeben durch

$$\varepsilon_1 = 1 - 4\theta - 10\theta^2 + 10\theta^3 + 15\theta^4 - 6\theta^5 - 7\theta^6 + \theta^7 + \theta^8,$$
$$\varepsilon_2 = 3\theta - \theta^4, \qquad \varepsilon_3 = 1 - 2\theta - 3\theta^2 + \theta^3 + \theta^4,$$
$$\varepsilon_4 = 2 - 9\theta^2 + 6\theta^4 - \theta^6, \qquad \varepsilon_5 = \theta,$$
$$\varepsilon_6 = 2 - \theta^2, \qquad \varepsilon_7 = 2 - 4\theta^2 + \theta^4,$$
$$\varepsilon_8 = -5\theta + 5\theta^2 + 10\theta^3 - 5\theta^4 - 6\theta^5 + \theta^6 + \theta^7.$$

Wir wollen alle Einheiten $\varepsilon \in \mathrm{U}_\mathscr{K}$ bestimmen, für welche auch jeweils $1 - \varepsilon$ eine Einheit aus $\mathrm{U}_\mathscr{K}$ ist. Dazu genügt es offensichtlich, in $\mathfrak{o}_\mathscr{K}$ die Einheitengleichung

$$1 \cdot a + 1 \cdot b = 1 \tag{1.21}$$

mit Koeffizienten $\alpha = 1 = \beta$ zu lösen.

Aus der Bakerschen Methode erhalten wir bei Verwendung der Linearform Λ'_μ aus 1.6 über $A_{2,\mu} = 10^{38}$ $(1 \leqslant \mu \leqslant 9)$ die obere Exponentenschranke $A = 10^{38}$ (zur Bestimmung von $A_{2,\mu}$ haben wir jeweils das minimale $x \in \mathbb{N}$ bestimmt, so daß (1.20) für $\bar{a} = 10^x$ nicht erfüllt ist). Wegen $\alpha = \beta$ ist natürlich ebenso $B = 10^{38}$. Die Rechenzeit zur Ermittlung von A betrug weniger als eine Sekunde.

1.2. *Reduktion der oberen Exponentenschranken*

Der zweite Schritt beim Lösen der Einheitengleichung (1.1) besteht darin, die oberen Exponentenschranken A und B *deutlich* zu reduzieren. Hierzu verwenden wir die im nächsten Lemma enthaltene Reduktionsmethode, welche im wesentlichen einer Arbeit von de Weger [26] entnommen ist, ergänzt um Überlegungen von Smart [23]. Wir formulieren das Vorgehen nur für die Reduktion von A, zur Reduktion von B kann analog verfahren werden.

LEMMA 1.8. *Zu beliebigem $\mu \in \mathscr{I}$ sei $K \in \mathbb{N}$ gegeben, so daß die Determinante*

$$\begin{vmatrix} 0 & \lfloor K\Re \operatorname{Log} \varepsilon_1^{(\mu)} \rceil \\ \left\lfloor K \dfrac{2\pi}{w} \right\rceil & \lfloor K\Im \operatorname{Log} \varepsilon_1^{(\mu)} \rceil \end{vmatrix} \neq 0, \tag{1.22}$$

und es sei $\Gamma = \Gamma_{\mu, K} \subset \mathbb{R}^{r+1}$ das Gitter, welches von den Spalten der Matrix

$$\begin{pmatrix} 0 & \lfloor K\Re \operatorname{Log} \varepsilon_1^{(\mu)} \rceil & \lfloor K\Re \operatorname{Log} \varepsilon_2^{(\mu)} \rceil & \cdots & \lfloor K\Re \operatorname{Log} \varepsilon_r^{(\mu)} \rceil \\ \left\lfloor K \dfrac{2\pi}{w} \right\rceil & \lfloor K\Im \operatorname{Log} \varepsilon_1^{(\mu)} \rceil & \lfloor K\Im \operatorname{Log} \varepsilon_2^{(\mu)} \rceil & \cdots & \lfloor K\Im \operatorname{Log} \varepsilon_r^{(\mu)} \rceil \\ 0 & 0 & 1 & & 0 \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & 0 & & 1 \end{pmatrix}, \tag{1.23}$$

erzeugt wird. Ferner sei $\tilde{z}_0, ..., \tilde{z}_r$ eine LLL-reduzierte Basis [15] von Γ.

(1) *Sei $\alpha \neq 1$ in (1.1). Es sei $z_\alpha \in \mathbb{Z}^{r+1}$ definiert durch*

$$z_\alpha^t = (\lfloor K\Re \operatorname{Log} \alpha^{(\mu)} \rceil, \lfloor K\Im \operatorname{Log} \alpha^{(\mu)} \rceil, 0, ..., 0),$$

und z_α habe die Darstellung

$$z_\alpha = \sum_{i=0}^{r} \alpha_i \tilde{z}_i \qquad (\alpha_0, ..., \alpha_r \in \mathbb{Q}),$$

wobei ein $j \in \{0, ..., r\}$ mit $\alpha_j \notin \mathbb{Z}$ existiere. Ist dieser Index j maximal gewählt, und ist ferner

$$\delta := |\alpha_j - \lfloor \alpha_j \rceil| \, 2^{-(r/2)} \, \|\tilde{z}_0\|_2 - \sqrt{2}(1 + A_{3,\mu} + rA_{2,\mu}) > 0, \tag{1.24}$$

so gelten für jedes $\alpha \in \mathfrak{L}_{\alpha,\mu}$ *mit* $\bar{a} \geqslant A_{1,\mu}$ *die Abschätzungen*

$$\bar{a} \leqslant \frac{1}{c_1} \log\left(\frac{3Kc_{2,\mu}}{2\delta}\right), \tag{1.25}$$

$$\bar{\bar{a}} \leqslant \frac{1}{c_3} \log\left(\frac{Kc_{4,\mu}}{\delta}\right). \tag{1.26}$$

(2) *Sei* $\alpha = 1$. *Ist*

$$\delta := 2^{-(r/2)} \|\tilde{z}_0\|_2 - \sqrt{2}(A_{3,\mu} + rA_{2,\mu}) > 0, \tag{1.27}$$

so gelten für jedes $a \in \mathfrak{L}_{\alpha,\mu}$ *mit* $\bar{a} \geqslant A_{1,\mu}$ *die Abschätzungen in* (1.25) *und* (1.26).

Wir erläutern kurz, wie anhand von 1.8 die obere Schranke A reduziert werden kann. Sei dazu $\mu \in \mathscr{I}$ beliebig, aber fest vorgegeben. Zur Verwendung von 1.8 benötigen wir zunächst ein geeignetes $K \in \mathbb{N}$. Aufgrund praktischer Erfahrung wählen wir $K = A_{2,\mu}^{r+1}$ (siehe auch [26, Chap. 3]). Ist dann die Bedingung (1.22) erfüllt, so bestimmen wir eine LLL-reduzierte Basis des Gitters $\Gamma_{\mu,K}$ und prüfen anschließend, ob δ der Bedingung (1.24) bzw. (1.27) genügt. Sofern letzteres der Fall ist, können wir $A_{2,\mu}$ und $A_{3,\mu}$ anhand von (1.25) und (1.26) ersetzen durch

$$\begin{aligned} A_{2,\mu} &\leftarrow \min\left(A_{2,\mu}, \left\lfloor \frac{1}{c_1}\left(\frac{3Kc_{2,\mu}}{2\delta}\right)\right\rfloor\right), \\ A_{3,\mu} &\leftarrow \min\left(A_{3,\mu}, \left\lfloor \frac{1}{c_3}\log\left(\frac{Kc_{4,\mu}}{\delta}\right)\right\rfloor\right). \end{aligned} \tag{1.28}$$

Diesen Reduktionsvorgang wiederholen wir solange, bis durch die Ersetzung in (1.28) keine weitere Verringerung von $A_{2,\mu}$ mehr eintritt. Nach Abschluß des Reduktionsvorgangs setzen wir dann

$$A := \max_{1 \leqslant \mu \leqslant r_1 + r_2} \max(A_{1,\mu}, A_{2,\mu}).$$

Bei diesem Reduktionsverfahren ist nicht gesichert, ob mit ihm überhaupt eine Reduktion der Schranken $A_{2,\mu}$ erreicht werden kann. Gleichwohl hat das Verfahren in der Praxis bei allen gerechneten Beispielen die gewünschte deutliche Reduktion der Ausgangsschranken bewirkt.

Bemerkung 1.9. (1) Die obere Schranke $A_{3,\mu}$ muß während des gesamten Reduktionsverfahrens mitverwaltet werden, um mit ihr den Koeffizienten a_0' in der Linearform abzuschätzen.

(2) Ist bei Wahl von $K = A_{2,\mu}^{r+1}$ die zur Reduktion notwendige Bedingung (1.24) bzw. (1.27) nicht erfüllt, so ersetzt man K durch einen größeren Wert und prüft nach erneuter LLL-Reduktion wiederum die Bedingung aus (1.24) bzw. (1.27). Iteriert man dieses Vorgehen, so hat sich in der Praxis gezeigt, daß für ein genügend großes K stets (1.24) bzw. (1.27) erfüllt werden kann. Sofern dann aus einem solchen K keine kleinere obere Schranke für $A_{2,\mu}$ in (1.28) resultiert, bricht man die Reduktion ab.

BEISPIEL 1.10 (Fortsetzung von 1.7). Setzen wir 1.8 zur Reduktion von $A_{2,1}$ ein, so bekommen wir durch wiederholte Anwendung von 1.8 schrittweise de Werte 14739, 2367, 2037 und 2031 als neue obere Schranken für $A_{2,1}$, wobei ein erneuter Reduktionsschritt keine weitere Verringerung der Schranke $A_{2,1} = 2031$ bewirkt. Für $A_{2,2}, ..., A_{2,9}$ liefert die wiederholte Reduktion mit 1.8 die neuen Schranken

$$A_{2,2} = 2026, \quad A_{2,3} = 2035, \quad A_{2,4} = 2076, \quad A_{2,5} = 2056,$$

$$A_{2,6} = 2028, \quad A_{2,7} = 2027, \quad A_{2,8} = 2029, \quad A_{2,9} = 2062.$$

Somit erhalten wir insgesamt die neue Schranke $A = 2076 = B$. Die Rechenzeit zur Reduktion der Schranken betrug 305s.

1.3. *Auszählen der Lösungen*

Nach Herleitung und Reduktion der oberen Exponentenschranke verbleibt als dritter und letzter Schritt die explizite Berechnung aller Lösungen der Einheitengleichung, also die Bestimmung von $\mathfrak{L}$. Dieser letzte Schritte ist der weitaus aufwendigste beim Lösen der Einheitengleichung. Ein naives systematisches Ausprobieren aller für $a \in \mathfrak{L}_\alpha$ und $b \in \mathfrak{L}_\beta$ in Frage kommenden Einheiten stößt bei Einheitenrang $r \geqslant 3$ schnell an die Grenze der praktischen Durchführbarkeit, da $w(2A+1)^r$ Möglichkeiten für $a \in \mathfrak{L}_\alpha$ und analog $w(2B+1)^r$ Möglichkeiten für $b \in \mathfrak{L}_\beta$ zu berücksichtigen sind. Als in der Praxis wesentlich effizienter erweist sich das folgende Verfahren, welches auf Methoden aus der Geometrie der Zahlen basiert.

Dieser Unterabschnitt ist in drei Teile gegliedert. Im ersten Teil werden einige technische Hilfsmittel bereitgestellt. Danach beschäftigen wir uns im zweiten Teil mit der speziellen Situation, daß die Koeffizienten α, β der Einheitengleichung (1.1) gegeben sind als $\alpha = 1 = \beta$. Gegenstand des dritten Teils ist abschließend die allgemeine Einheitengleichung mit beliebigen $\alpha, \beta \in \mathscr{K}^\times$.

1.3.1. *Technische Hilfsmittel.* Wir fixieren einige Notationen. Für $s > 1$ setzen wir

$$\ll s \gg := \left\{ (x_1, ..., x_{r_1+r_2})^t \in \mathbb{R}^{r_1+r_2} \;\middle|\; \frac{1}{s} \leqslant x_i \leqslant s \; (i \in \mathscr{I}) \right\}. \tag{1.29}$$

Wir sagen, daß $\gamma \in \mathscr{K}$ in $M \subseteq \mathbb{R}^{r_1+r_2}$ liegt, und schreiben dafür kurz $\gamma \in M$, sofern

$$(|\gamma^{(1)}|, ..., |\gamma^{(r_1+r_2)}|)^t \in M.$$

Sind $j \in \mathscr{I}$, $\rho \in \mathscr{K}^\times$, $\delta \in (0, 1)$ und $s > 1$ gegeben, so sei $U_j(\rho, \delta, s) \subseteq \mathrm{U}_{\mathscr{K}}$ definiert als

$$U_j(\rho, \delta, s) := \{ \varepsilon \in \mathrm{U}_{\mathscr{K}} \mid |(\rho\varepsilon)^{(j)} - 1| < \delta \wedge \rho\varepsilon \in \ll s \gg \}. \tag{1.30}$$

Zur späteren Verwendung notieren wir ein einfaches Lemma.

LEMMA 1.11. *Sei $\mathscr{K}$ normal über $\mathbb{Q}$ (also $r_1 = 0$ oder $r_2 = 0$), seien $\rho \in \mathbb{Q}$, $\delta \in (0, 1)$ sowie $s > 1$. Dann operiert die Galoisgruppe von $\mathscr{K}/\mathbb{Q}$ transitiv auf $\{ U_j(\rho, \delta, s) \mid j \in \mathscr{I} \}$.*

Die Mengen $U_j(\rho, \delta, s)$ aus (1.30) werden die entscheidende Rolle bei der expliziten Berechnung aller Lösungen der Einheitengleichung (1.1) spielen. Wir beschreiben im folgenden, wie die Elemente dieser Mengen bestimmt werden können. Hierzu benötigen wir ein technisches Lemma.

LEMMA 1.12. *Seien $\delta \in (0, 1)$, $s > 1$ und $z \in \mathbb{C}$.*

(1) *Ist $|z - 1| \leqslant \delta$, so gilt $|\log |z|| \leqslant \log(1/1 - \delta)$.*

(2) *Ist $|z| \in [1/s, s]$, so gilt $|\log |z|| \leqslant \log s$.*

(3) *Ist $|z - 1| \leqslant \delta$, so gilt $|\operatorname{Arg} z| \leqslant \arccos \sqrt{1 - \delta^2}$.*

Seien j, ρ, δ, s wie bei der Definition von $U_j(\rho, \delta, s)$ in (1.30) gegeben. Definiere $\lambda_0, ..., \lambda_{r_1+r_2} > 0$ durch

$$\lambda_0 := \frac{1}{\arccos \sqrt{1 - \delta^2}}, \quad \lambda_i := \frac{1}{\log s} \; (i \in \mathscr{I}, i \neq j), \quad \lambda_j := \frac{1}{\log \dfrac{1}{1 - \delta}},$$

und damit weiter die Abbildung

$$L_\lambda \colon \mathscr{K}^\times \to \mathbb{R}^{r_1+r_2+1} \colon x \mapsto \begin{pmatrix} \lambda_0 \operatorname{Arg} x^{(j)} \\ \lambda_1 \log |x^{(1)}| \\ \vdots \\ \lambda_{r_1+r_2} \log |x^{(r_1+r_2)}| \end{pmatrix}. \tag{1.31}$$

Gemäß 1.12 gilt für jedes $\varepsilon \in U_j(\rho, \delta, s)$ die Abschätzung

$$\|L_\lambda(\rho\varepsilon)\|_2^2 = \lambda_0^2 \operatorname{Arg}^2(\rho\varepsilon)^{(j)} + \sum_{i=1}^{r_1+r_2} \lambda_i^2 \log^2 |(\rho\varepsilon)^{(i)}| \leqslant r_1 + r_2 + 1. \quad (1.32)$$

Es bezeichne Λ_λ das $(r+1)$-dimensionale Gitter in $\mathbb{R}^{r_1+r_2+1}$, welches von den Vektoren $v = (2\pi/w, 0, ..., 0)^t$ und $L_\lambda(\varepsilon_1), ..., L_\lambda(\varepsilon_r)$ aufgespannt wird. Wir setzen

$$V(\rho, \lambda) := \left\{ x \in \Lambda_\lambda \;\middle|\; \left\| x - L_\lambda\left(\frac{1}{\rho}\right) \right\|_2^2 \leqslant r_1 + r_2 + 1 \right\}. \quad (1.33)$$

Ist $\varepsilon = \xi\varepsilon^{e_1} \cdots \varepsilon^{e_r} \in U_j(\rho, \delta, s)$, so existiert $e_0 \in \mathbb{Z}$ mit

$$L_\lambda(\rho\varepsilon) = \underbrace{e_0 v + e_1 L_\lambda(\varepsilon_1) + \cdots + e_r L_\lambda(\varepsilon_r)}_{=: e \in \Lambda_\lambda} + L_\lambda(\rho).$$

Wegen $L_\lambda(\rho) = -L_\lambda(1/\rho)$ gilt nach (1.32) also $e \in V(\rho, \lambda)$. Damit erhält man alle Einheiten aus $U_j(\rho, \delta, s)$ leicht aus den Elementen der Menge $V(\rho, \lambda)$. Diese entsprechen gerade den Gitterpunkten von Λ_λ, welche innerhalb eines Ellipsoids mit Mittelpunkt $L_\lambda(1/\rho)$ liegen. Daher ist $V(\rho, \lambda)$ endlich und kann mit dem Auszählalgorithmus von Fincke und Pohst [5, 21] bestimmt werden.

Bemerkung 1.13. Ist $N(\rho) \neq \pm 1$, so berechnet man zur Anwendung des Auszählalgorithmus von Fincke und Pohst zunächst die orthogonale Projektion p des Punktes $L_\lambda(1/\rho)$ in den von Λ_λ erzeugten $(r+1)$-dimensionalen Unterraum des $\mathbb{R}^{r_1+r_2+1}$ und bestimmt anschließend mit dem Auszählalgorithmus alle Gitterpunkte $x \in \Lambda_\lambda$ mit $\|x - p\|_2^2 \leqslant r_1 + r_2 + 1$. Gilt $\|L_\lambda(1/\rho) - p\|_2^2 > r_1 + r_2 + 1$, so ist natürlich $V(\rho, \lambda) = \varnothing$, also auch $U_j(\rho, \delta, s) = \varnothing$.

Bevor wir uns in den nächsten beiden Teilen der expliziten Berechnung aller Lösungen der Einheitengleichung zuwenden, vermerken wir, daß für $s > 1$ alle Einheiten ε in $\langle\langle s \rangle\rangle$ mit dem Auszählalgorithmus von Fincke und Pohst berechnet werden können, denn für jedes solche ε gilt

$$\sum_{i=1}^{r_1+r_2} \frac{1}{\log^2 s} \log |\varepsilon^{(i)}|^2 \leqslant r_1 + r_2. \quad (1.34)$$

1.3.2. *Ausnahmeeinheiten.* Wie bereits angekündigt, werden wir bei der expliziten Berechnung aller Lösungen der Einheitengleichung (1.1)

zunächst den Spezialfall betrachten, daß die Koeffizienten gegeben sind durch $\alpha = 1 = \beta$. Der Grund für die gesonderte Behandlung dieses Spezialfalls ist einerseits die Tatsache, daß das Lösungsverfahren für diesen Fall einfacher und auch effizienter ist als im allgemeinen Fall. Auf der anderen Seite ist der Fall $\alpha = 1 = \beta$ von besonderem Interesse, wie wir später kurz erläutern werden. Wir definieren zunächst den auf Nagell zurückgehenden Begriff der *Ausnahmeeinheit*.

DEFINITION 1.14. Eine Einheit $\varepsilon \in \mathrm{U}_{\mathscr{K}}$ heißt Ausnahmeeinheit von $\mathscr{K}$, falls $1-\varepsilon$ ebenso eine Einheit aus $\mathrm{U}_{\mathscr{K}}$ ist.

Die Menge der Ausnahmeeinheiten von $\mathscr{K}$ bezeichnen wir mit $\mathrm{X}_{\mathscr{K}}$. Ist $\varepsilon \in \mathrm{X}_{\mathscr{K}}$, so nennen wir

$$\Omega(\varepsilon) := \left\{\varepsilon, \frac{1}{\varepsilon}, 1-\varepsilon, 1-\frac{1}{\varepsilon}, \frac{1}{1-\varepsilon}, \frac{\varepsilon}{\varepsilon-1}\right\}$$

den *Orbit* von ε. Für eine Ausnahmeeinheit $\varepsilon \in \mathrm{X}_{\mathscr{K}}$ gilt stets $\Omega(\varepsilon) \subseteq \mathrm{X}_{\mathscr{K}}$, und es ist

$$|\Omega(\varepsilon)| = \begin{cases} 2: & \varepsilon \text{ ist eine primitive sechste Einheitswurzel} \\ 6: & \text{sonst.} \end{cases}$$

Die Bestimmung von $\mathrm{X}_{\mathscr{K}}$ is äquivalent zum Lösen der Einheitengleichung $a+b=1$. Zu dieser Einheitengleichung seien obere Exponentenschranken $A = B$ gegeben, wie wir sie bereits bestimmt haben. Wir setzen

$$\bar{S} := \max_{i \in \mathscr{I}} \exp\left(A \sum_{j=1}^{r} |\log |\varepsilon_j^{(i)}||\right). \tag{1.35}$$

Für jedes $\varepsilon \in \mathrm{X}_{\mathscr{K}}$ gilt $\varepsilon \in \langle\langle \bar{S} \rangle\rangle$ oder $1-\varepsilon \in \langle\langle \bar{S} \rangle\rangle$, in jedem Fall also $|\varepsilon^{(i)}| \leqslant \bar{S}+1 (i \in \mathscr{I})$, und weiter

$$\mathrm{X}_{\mathscr{K}} \subseteq \langle\langle \bar{S}+1 \rangle\rangle, \tag{1.36}$$

da für $\varepsilon \in \mathrm{X}_{\mathscr{K}}$ auch stets $1/\varepsilon \in \mathrm{X}_{\mathscr{K}}$ ist.

Das entscheidende Hilfsmittel zur Berechnung von $\mathrm{X}_{\mathscr{K}}$ ist das nachfolgende Lemma, in dem für $X \subseteq \mathrm{X}_{\mathscr{K}}$ die Menge $\Omega(X)$ definiert sei als

$$\Omega(X) := \bigcup_{\varepsilon \in X} \Omega(\varepsilon).$$

LEMMA 1.15. *Es seien* $S>1$ *und* $X\subseteq \mathrm{X}_{\mathscr{K}}$ *gegeben mit*

$$\mathrm{X}_{\mathscr{K}} \subseteq \langle\!\langle S\rangle\!\rangle \cup \Omega(X). \tag{1.37}$$

Ferner sei $s>1$ *beliebig mit* $s\leqslant S$.

Mit $T := U_1(1, 1/s, S) \cup ... \cup U_{r_1+r_2}(1, 1/s, S)$ *gilt dann*

$$\mathrm{X}_{\mathscr{K}} \subseteq \langle\!\langle s\rangle\!\rangle \cup \Omega(X \cup (T \cap \mathrm{X}_{\mathscr{K}})).$$

Beweis. Sei $\varepsilon\in \mathrm{X}_{\mathscr{K}}$ beliebig. Gilt $\varepsilon\in \langle\!\langle s\rangle\!\rangle \cup \Omega(X)$, so ist nichts zu zeigen. Sei also $\varepsilon\notin \langle\!\langle s\rangle\!\rangle \cup \Omega(X)$. Indem wir gegebenenfalls ε durch $1/\varepsilon\in \mathrm{X}_{\mathscr{K}}$ ersetzen, können wir ohne Einschränkung annehmen, daß $j\in\mathscr{J}$ mit $|\varepsilon^{(j)}|>s$ existiert. Für $\eta := 1-(1/\varepsilon)\in \mathrm{X}_{\mathscr{K}}$ gilt dann

$$|\eta^{(j)}-1| = \left|\frac{1}{\varepsilon^{(j)}}\right| < \frac{1}{s}.$$

Aus $\eta\in\Omega(\varepsilon)$ und $\varepsilon\notin\Omega(X)$ folgt gemäß der Voraussetzung $\eta\in\langle\!\langle S\rangle\!\rangle$, also

$$\frac{1}{S}\leqslant |\eta^{(i)}|\leqslant S \qquad (i\in\mathscr{J}).$$

Somit $\eta\in U_j(1, 1/s, S)$, also $\varepsilon\in\Omega(\eta)\subseteq\Omega(T\cap \mathrm{X}_{\mathscr{K}})$. ∎

Die Grundidee bei der Berechnung von $\mathrm{X}_{\mathscr{K}}$ ist jetzt wie folgt: Wir geben uns zuerst ein $m\in\mathbb{N}_0$ sowie $S_0>S_1>...>S_m>1$ vor und berechnen anschließend schrittweise endliche Mengen $X_0, ..., X_m\subseteq \mathrm{X}_{\mathscr{K}}$ so, daß für jedes $k\in\{0, ..., m\}$ die Implikation

$$\varepsilon\in \mathrm{X}_{\mathscr{K}} \Rightarrow \varepsilon\in\Omega(X_k) \vee \varepsilon\in\langle\!\langle S_k\rangle\!\rangle \tag{1.38}$$

erfüllt ist.

Dazu setzen wir $S_0 := \bar{S}+1$ und $X_0 := \varnothing$. Die Implikation (1.38) entspricht dann gerade (1.36). Wir wollen nun davon ausgehen, daß wir $m\in\mathbb{N}_0$ und $S_1, ..., S_m>1$ bereits vorgegeben haben, und erläutern jetzt die Konstruktion von $X_1, ..., X_m$. Wie m und $S_1, ..., S_m$ in der Praxis zu wählen sind, beschreiben wir weiter unten. Ist für $k\in\{0, ..., m-1\}$ die Menge X_k bekannt, so berechnen wir $T\subseteq \mathrm{U}_{\mathscr{K}}$ aus 1.15, wobei dort jetzt $s=S_{k+1}$ und $S=S_k$, und setzen

$$X_{k+1} := X_k \cup (T\cap \mathrm{X}_{\mathscr{K}}).$$

Aufgrund von 1.15 ist die geforderte Implikation (1.38) erfüllt.

Unser Vorgehen fassen wir in einem kurzen Algorithmus zur Berechnung von $X_{\mathscr{K}}$ zusammen.

ALGORITHMUS 1.16.
Eingabe: *Ein algebraischer Zahlkörper* $\mathscr{K}$, $m \in \mathbb{N}_0$ *und* $S_0 > S_1 > \cdots > S_m > 1$ *mit* $X_{\mathscr{K}} \subseteq \langle\langle S_0 \rangle\rangle$.
Ausgabe: $X_{\mathscr{K}}$.
Schritt 1
$X_0 \leftarrow \varnothing$.
Schritt 2 (Konstruktion von $X_1, ..., X_m$)
`foreach` $k \in \{1, ..., m\}$ `do`
$X_k \leftarrow X_{k-1}$.
`foreach` $j \in \mathscr{I}$ `do`
Bestimme durch Auszählen die Menge $X_{k,j}$ aller Ausnahmeeinheiten in $U_j(1, 1/S_k, S_{k-1})$ und setze $X_k \leftarrow X_k \cup X_{k,j}$.
`end`
`end`
Schritt 3 (Ausnahmeeinheiten in $\langle\langle S_m \rangle\rangle$)
Bestimme durch Auszählen (vergleiche (1.34)) die Menge X'_{m+1} aller Ausnahmeeinheiten in $\langle\langle S_m \rangle\rangle$.
Schritt 4
Setze $X_{\mathscr{K}} \leftarrow \Omega(X_m) \cup X'_{m+1}$ und terminiere.

Anhand einer Betrachtung zur Komplexität von Algorithmus 1.16 werden wir jetzt die Wahl von m und $S_1, ..., S_m$ in der Praxis beschreiben.

Liegt eine Einheit $\varepsilon \in U_{\mathscr{K}}$ in einer der im zweiten Schritt von 1.16 durch Auszählen zu bestimmenden Mengen $U_j(1, 1/S_k, S_{k-1})$, so gelten für ε gemaß 1.12 die Abschätzungen

$$|\log |\varepsilon^{(j)}|| \leqslant \log \frac{S_k}{S_k - 1}, \qquad |\log |\varepsilon^{(i)}|| \leqslant \log S_{k-1} \quad (i \in \mathscr{I}).$$

Es ist also der Vektor $(\log |\varepsilon^{(1)}|, ..., \log |\varepsilon^{(r_1+r_2)}|)^t$ in einem Quader des $\mathbb{R}^{r_1+r_2}$ mit Volumen $2^{r+1} \log(S_k/S_k - 1) \log^r S_{k-1}$ gelegen. Wir wollen daher im folgenden annehmen, daß der Aufwand für das Auszählen aller in $U_j(1, 1/S_k, S_{k-1})$ gelegenen Einheiten proportional zu $\log(S_k/S_k - 1) \log^r S_{k-1}$ ist (der nur von r abhängige Faktor 2^{r+1} beim Quadervolumen ist für unsere Betrachtungen ohne Bedeutung).

Im dritten Schritt von 1.16 müssen alle Einheiten $\varepsilon \in U_{\mathscr{K}}$ ausgezählt werden, welche in $\langle\langle S_m \rangle\rangle$ liegen. Da für jedes solche ε die Abschätzung

$|\log|\varepsilon^{(i)}||\leqslant \log S_m$ $(i\in\mathscr{I})$ erfüllt ist, setzen wir den Aufwand für die Durchführung des dritten Schrittes von 1.16 entsprechend mit $\log^{r+1} S_m$ an.

Der Gesamtaufwand von Algorithmus 1.16 ist bei den gemachten Annahmen also proportional zu

$$F_m(S_0; S_1, ..., S_m) := (r+1)\sum_{k=1}^{m} \log\frac{S_k}{S_k-1}\log^r S_{k-1} + \log^{r+1} S_m. \tag{1.39}$$

Im Hinblick auf die Effizienz sind also $m\in\mathbb{N}_0$ und $S_1>...>S_m>1$ so zu wählen, daß $F_m(S_0; S_1, ..., S_m)$ unter der Nebenbedingung $S_1<S_0$ klein wird. Im folgenden beschreiben wir, wie wir in der Praxis $S_1, ..., S_m$ gewählt haben. Wir fixieren zunächst m und betrachten die Funktion

$$f: V\to\mathbb{R}: (x_1, ..., x_m)^t\mapsto F_m(S_0; x_1, ..., x_m),$$

wobei $V:=\{x\in\mathbb{R}^m \mid x_i>1 (1\leqslant i\leqslant m)\}$. Sei $S=(S_1, ..., S_m)\in V$ eine lokale Minimalstelle von f. Da der Gradient von f in S verschwindet, folgt für jedes $i\in\{1, ..., m-1\}$ über

$$\frac{\partial f}{\partial x_i}(S_1, ..., S_m) = (r+1)\left(\left(\frac{1}{S_i}-\frac{1}{S_i-1}\right)\log^r S_{i-1} + \log\frac{S_{i+1}}{S_{i+1}-1}\,\frac{r\log^{r-1} S_i}{S_i}\right)$$

die rekursive Beziehung

$$S_{i+1}=\frac{g(S_i)}{g(S_i)-1}, \quad \text{wo} \quad g(S_i):=\exp\left(\frac{\log^r S_{i-1}}{r(S_i-1)\log^{r-1} S_i}\right). \tag{1.40}$$

Es ist ferner

$$0=\frac{\partial f}{\partial x_m}(S_1, ..., S_m) = (r+1)\left(\left(\frac{1}{S_m}-\frac{1}{S_m-1}\right)\log^r S_{m-1} + \frac{\log^r S_m}{S_m}\right), \tag{1.41}$$

wobei wir die rechte Seite in (1.41) anhand von (1.40) als eine Funktion h in S_1 auffassen können.

Zur Bestimmung der lokalen Mimimalstellen von f genügt es demnach, wenn wir jede Nullstelle S_1 von h im Intervall $(1, +\infty)$ ermitteln und anschließend überprüfen, ob für die aus S_1 vermöge (1.40) resultierenden Werte $S_2, ..., S_m$ die Hessesche-Matrix von f an der Stelle $(S_1, ..., S_m)$ positiv definit ist.

Bei den in der Praxis aufgetretenen Werten von S_0—zumeist $S_0 > 10^r$—lassen numerische Untersuchungen vermuten, daß h im Intervall $(1 + \infty)$ stets genau einer Nullstelle S_1 besitzt. In allen gerechneten Fällen korrespondierte S_1 zu einer lokalen Minimalstelle $(S_1, ..., S_m)^t$ von f, für welche zusätzlich $S_1 > ... > S_m$ galt.

Nachdem wir die Wahl von $S_1, ..., S_m$ beschrieben haben, müssen wir nun noch m festlegen. Dazu betrachten wir die folgende Tabelle, welche für einige Werte von m und r den jeweils entsprechenenden Wert $F_m(S_0; S_1, ..., S_m)$ and der mit obigem Verfahren numerisch berechneten lokalen Minimalstelle $(S_1, ..., S_m)^t \in V$ wiedergibt, wobei für $S_0 = 10^{10r}$ dort stets $S_1 < S_0$ erfüllt ist (da wir m jetzt variieren, werden wir von nun an gelegentlich korrektor $(S_1(m), ..., S_m(m))$ schreiben).

m	$r=2$	$r=3$	$r=4$	$r=5$	$r=6$
0	97664.57	$2.28 \cdot 10^7$	$6.63 \cdot 10^9$	$2.33 \cdot 10^{12}$	$9.61 \cdot 10^{14}$
1	102.66	2113.26	56712.77	$1.87 \cdot 10^6$	$7.36 \cdot 10^7$
2	16.54	136.28	1540.35	22009.94	$3.79 \cdot 10^5$
3	8.72	46.37	344.06	3267.78	37750.99
4	6.72	28.13	165.44	1252.33	11576.74
5	6.01	21.83	111.53	735.35	5932.61
6	5.75	19.10	89.09	536.94	3964.05
7	5.67	17.80	78.08	442.74	3076.11
8	5.65	17.18	72.22	392.35	2611.37
9	5.64	16.89	69.00	363.55	2345.53
10	5.64	16.78	67.24	346.57	2185.36

In der Praxis haben wir m jeweils so gewählt, daß die von m abhängige Funktion h eine Nullstelle in $(1, S_0)$ besitzt und darüber hinaus $F_m(S_0; S_1(m), ..., S_m(m)) < 0.9 \cdot F_{m-1}(S_0; S_1(m-1), ..., S_{m-1}(m-1))$ gilt. Der zweiten Bedingung liegt die Beobachtung zugrunde, daß ein noch größeres m den mit $F_m(S_0; S_1(m), ..., S_m(m))$ angesetzten Aufwand von Algorithmus 1.16 zwar weiter geringfügig reduziert, andererseits aber der Verwaltungsaufwand für das Auszählen linear in m zunimmt.

Die Diskussion zur Wahl von m und $S_1, ..., S_m$ beschließen wir mit einer zweiten Tabelle, welche bei diesmal festem Einheitenrang $r = 5$ aufzeigt,

wie sich die Größe der Ausgangsschranke S_0 auf die Werte von $F_m(S_0; S_1(m), ..., S_m(m))$ auswirkt.

S_0	$m=5$	$m=10$	$m=15$	$m=20$
10^{10}	539.46	335.26	323.99	323.85
10^{20}	639.17	341.72	324.30	323.85
10^{50}	735.35	346.57	324.53	323.85
10^{100}	791.66	349.04	324.65	323.85
10^{500}	890.44	352.88	324.85	323.86
10^{1000}	923.91	354.07	324.92	323.86
10^{5000}	988.24	356.24	325.04	323.86

Wir entnehmen dieser Tabelle, daß die Größe der Ausgangsschranke für die Komplexität von 1.16 nur von untergeordneter Bedeutung zu sein scheint (für andere Einheitenränge ergibt sich ein ähnliches Bild).

Bemerkung 1.17. Für $m=0$ entspricht Algorithmus 1.16 annähernd dem eingangs erwähnten naiven systematischen Auszählen aller Lösungen der Einheitengleichung. Aus der ersten Tabelle ersehen wir, warum das vorgestellte Verfahren bei passender Wahl von m weitaus effizienter ist.

Der Anwendung von Algorithmus 1.16 auf das in 1.7 begonnene Beispiel stellen wir zwei Bemerkungen voran.

Bemerkung 1.18. Sei $\mathcal{K}$ normal über $\mathbb{Q}$ mit Galoisgruppe G. Dann genügt in Schritt 2 von 1.16 die Bestimmung von $X_{1,1}, ..., X_{m,1}$, d.h. der in

$$U_1\left(1, \frac{1}{S_1}, S_0\right) \cup \cdots \cup U_1\left(1, \frac{1}{S_m}, S_{m-1}\right)$$

liegenden Ausnahmeeinheiten, da wir wegen 1.11 jede Menge $X_{k,j}$ $(2 \leqslant j \leqslant r_1 + r_2)$ anhand eines passenden $\sigma \in G$ erhalten können aus $X_{k,j} = \sigma(X_{k,1})$. Dementsprechend entfällt in (1.39) der Faktor $r+1$ vor dem Summenzeichen.

Bemerkung 1.19. In den Schritten 2 und 3 von 1.16 ist für jede der ausgezählten Einheiten ε zu testen, ob ε eine Ausnahmeeinheit ist. Weil es sich erfahrungsgemäß bei der Mehrzahl der ausgezählten Einheiten nicht um Ausnahmeeinheiten handelt, kann die Laufzeit von 1.16 merklich dadurch reduziert werden, indem man ein Testverfahren einsetzt, welches schnell Nicht-Ausnahmeeinheiten erkennt. Ein solches Verfahren wird von Smart in [23] erläutert.

BEISPIEL 1.20 (Fortsetzung von 1.7 und 1.10). Die eingangs in 1.7 formulierte Aufgabe entspricht gerade der Berechnung von $X_{\mathscr{K}}$. Mit der oberen Exponentenschranke $A = 2076$ aus 1.10 erhalten wir über (1.35) zunächst $S_0 = 6.9 \cdot 10^{4843}$. Da $\mathscr{K}$ normal ist, können wir 1.18 mit der dort beschriebenen Modifikation von F_m einsetzen. Es ist

$$F_9(S_0; S_1, ..., S_9) = 172680.33$$

$$F_{10}(S_0; S_1, ..., S_{10}) = 179210.18$$

$$F_{11}(S_0; S_1, ..., S_{11}) = 134811.60$$

$$F_{12}(S_0; S_1, ..., S_{12}) = 125593.54,$$

und bei Verwendung von $m = 10$ erhalten wir

$$S_1 = 1.49 \cdot 10^{30}, \quad S_2 = 3.89 \cdot 10^{11}, \quad S_3 = 5.52 \cdot 10^7, \quad S_4 = 982337.37,$$

$$S_5 = 73360.74, \quad S_6 = 9896.88, \quad S_7 = 1780.14, \quad S_8 = 365.36,$$

$$S_9 = 74.25, \quad S_{10} = 11.47.$$

Benutzen wir diese Werte in Algorithmus 1.16, so ergeben sich dort in Schritt 2 die folgende Rechenzeiten.

k	$\log \frac{S_k}{S_k - 1} \log^8 S_k$	t
1	160.83	2*s*
2	1396.70	2*s*
3	4659.05	14*s*
4	10831.82	48*s*
5	17905.66	97*s*
6	25075.13	160*s*
7	28837.78	224*s*
8	26986.93	275*s*
9	19933.12	203*s*
10	10805.69	147*s*

Die Rechenzeit für Schritt 3 ($\log^9 S_{10} = 3067.47$) betrug 25*s*, und insgesamt ergab sich eine Rechenzeit von 1555s für die Berechnung von $X_{\mathscr{K}}$. Auf die Wiedergabe der 28398 Ausnahmeeinheiten in $\mathscr{K}$ sei hier verzichtet.

Man kann das Ergebnis aus Beispiel 1.20 einsetzen, um anhand des folgenden Lemmas von Győry [13, Lemme 12] leicht alle Ausnahmeeinheiten in $\mathbb{Q}(\zeta_{19})$ zu berechnen.

LEMMA 1.21 (Győry). *Sei $\mathscr{K}$ ein CM-Körper. Dann besitzt jede nicht-reelle Ausnahmeeinheit von $\mathscr{K}$ die Gestalt*

$$\frac{1-\xi_2}{\xi_1-\xi_2}$$

mit Einheitswurzeln $\xi_1, \xi_2 \in \mathrm{TU}_{\mathscr{K}}$.

In Verbindung mit 1.21 haben wir mit unserem Verfahren die Ausnahmeeinheiten in allen Kreisteilungskörpern vom Grad $\leqslant 22$ bestimmt. Die Ergebnisse sind in der folgenden Tabelle aufgelistet. Für eine primitive m-te Einheitswurzel ζ_m mit $m \in \mathbb{N}$, $m \not\equiv 2 \bmod 4$, bezeichnet dort $\mathscr{K}_m$ den Kreisteilungskörper $\mathbb{Q}(\zeta_m)$ mit maximalem reellen Teilkörper $\mathscr{K}_m^+$. Wir haben jeweils zuerst die Ausnahmeeinheiten in $\mathscr{K}_m^+$ bestimmt (Rechenzeit t_1) und diese dann mit 1.21 zur Menge aller Ausnahmeeinheiten in $\mathscr{K}_m^+$ erweitert. Die Rechenzeit t_2 zeigt lediglich die zur Einbettung von $X_{\mathscr{K}_m^+}$ in $\mathscr{K}_m$ und der Anwendung von 1.21 benötigte Zeit an. Da für $m = 8, 16, 24, 32, 48$ ein Primideal der Norm 2 in $\mathfrak{o}_{\mathscr{K}_m^+}$ existiert, ist $X_{\mathscr{K}_m^+}$ in diesem Fall leer, wodurch sich die Rechenzeiten von 0 Sekunden in der Tabelle I erklären. Der Fall $m = 23$ mit Einheitenrang 10 zeigt die Grenzen unseres Verfahrens auf.

TABELLE I

m	$[\mathscr{K}_m^+ : \mathbb{Q}]$	$\lvert X_{K_m^+}\rvert$	t_1	$[\mathscr{K}_m : \mathbb{Q}]$	$\lvert X_{K_m}\rvert$	t_2
1	1	0	0s	1	0	0s
3	1	0	0s	2	2	0s
4	1	0	0s	2	0	0s
5	2	6	0s	4	18	0s
7	3	42	1s	6	72	0s
8	2	0	0s	4	0	0s
9	3	18	1s	6	38	0s
11	5	570	4s	10	660	0s
12	2	0	0s	4	14	0s
13	6	1830	14s	12	1962	2s
15	4	90	1s	8	440	1s
16	4	0	0s	8	0	0s
17	8	11700	246s	16	11940	30s
19	9	28398	1492s	18	28704	128s

TABELLE I (*continued*)

m	$[\mathscr{K}_m^+ : \mathbb{Q}]$	$\lvert X_{K_m^+}\rvert$	t_1	$[\mathscr{K}_m : \mathbb{Q}]$	$\lvert X_{K_m}\rvert$	t_2
20	4	54	1s	8	138	0s
21	6	1416	16s	12	2192	6s
23	11	130812	160941s	22	131274	47026s
24	4	0	0s	8	86	0s
25	10	47766	12405s	20	48078	332s
27	9	8676	1096s	18	8858	32s
28	6	678	15s	12	888	2s
32	8	0	0s	16	0	0s
33	10	73110	16635s	20	75242	514s
36	6	354	14s	12	710	3s
40	8	4398	196s	16	4914	14s
44	10	30030	7335s	20	30660	133s
48	8	0	0s	16	422	16s
60	8	14274	275s	16	16340	46s

Wir hatten eingangs geäußert, daß das Lösen der Einheitengleichung $a+b=1$, d.h. der Berechnung aller Ausnahmeeinheiten, von besonderem Interesse ist. Dies werden wir jetzt kurz erläutern, wobei wir uns auf eine Arbeit von Niklasch [20] stützen.

Für einen Zahlkörper $\mathscr{K}$ vorgegebener Signatur (n, r), d.h., $\mathscr{K}$ besitzt den Grad n und Einheitenrang r, ist nach einem Resultat von Evertse [4] die Anzahl der Ausnahmeeinheiten von $\mathscr{K}$ nach oben begrenzt durch $|X_{\mathscr{K}}| \leqslant 3 \cdot 7^{n+2r+2}$. Es existiert also eine nur von (n, r) abhängige Konstante

$$C_1(n, r) := \max\{|X_{\mathscr{K}}| \mid \mathscr{K} \text{ ein algebraischer Zahlkörper der Signatur } (n, r)\}.$$

Für $r \leqslant 1$ wird $C_1(n, r)$ jeweils von dem Körper angenommen, welcher innerhalb der Signatur die kleinste Absolutdiskriminante besitzt [17, 18]. Für $r > 1$ sind die exakten Werte von $C_1(n, r)$ bislang unbekannt. Allerdings lassen umfangreiche Beispielrechnungen, die wir mit unserem Verfahren durchgeführt haben [27], vermuten, daß die Situation ähnlich wie bei den Einheitenrängen 0 und 1 ist. Innerhalb einer Signatur scheinen es stets Körper mit kleiner Absolutdiskriminante zu sein, welche über die meisten Ausnahmeeinheiten verfügen. Die folgende Tabelle II enthält für Körpergrade $n \leqslant 8$ und Einheitenrang $r \in \{2, ..., n-1\}$ jeweils die Anzahl der Ausnahmeeinheiten der—soweit bekannt—fünf Körper kleinster Absolutdiskriminante zur Signatur (n, r).

TABELLE II

r	n	$\lvert X_{\mathscr{K}}\rvert$ (disc$_{\mathscr{K}}$)
2	3	42 (49), 18 (81), 0 (148), 12 (169), 0 (229)
2	4	54 (−275), 54 (−283), 42 (−331), 30 (−400), 30 (−448)
2	5	78 (1609), 78 (1649), 72 (1777), 54 (2209), 48 (2297)
2	6	110 (−9747), 102 (−10051), 96 (−10571), 96 (−10816), 86 (−11691)
3	4	162 (725), 90 (1125), 54 (1600), 36 (1957), 54 (2000)
3	5	228 (−4511), 198 (−4903), 180 (−5519), 168 (−5783), 132 (−7031)
3	6	288 (28037), 282 (29077), 282 (29189), 270 (30125), 258 (31133)
3	7	366 (−184607), 348 (−193327), 348 (−193607), 342 (−196127), 336 (−199559)
3	8	438 (1257728), 440 (1265625), 432 (1282789), 434 (1327833), 422 (1342413)
4	5	570 (14641), 336 (24217), 138 (36497), 240 (38569), 78 (65657)
4	6	750 (−92779), 744 (−94363), 696 (−103243), 666 (−104483), 684 (−104875)
4	7	954 (612233), 960 (612569), 912 (640681), 906 (649177), 882 (661033)
5	6	2070 (300125), 1830 (371293), 1542 (434581), 1416 (453789), 1380 (485125)
5	7	2310 (−2306599), 2286 (−2369207), 2112 (−2616839), 1980 (−2790047), 1998 (−2790551)
6	7	2892 (20134393), 1320 (25164057), 2652 (25367689), 2118 (28118369), 1146 (30653489)
7	8	15804 (282300416), 14742 (309593125), 14274 (324000000)

1.3.3. *Allgemeine Einheitengleichungen.* Nachdem wir zur Bestimmung aller Lösungen der Einheitengleichung $a+b=1$ Methoden aus der Geometrie der Zahlen eingesetzt haben, formulieren wir jetzt ein ähnliches Verfahren für die allgemeine Einheitengleichung $\alpha a+\beta b=1$ mit beliebigen $\alpha, \beta \in \mathscr{K}^{\times}$.

Unter Verwendung der oberen Exponentenschranken A und B setzen wir analog zu (1.35) zunächst

$$\bar{A} := \max_{i \in \mathscr{I}} \exp\left(A \sum_{j=1}^{r} |\log |\varepsilon_j^{(i)}||\right),$$

$$\bar{B} := \max_{i \in \mathscr{I}} \exp\left(B \sum_{j=1}^{r} |\log |\varepsilon_j^{(i)}||\right),$$

also $\mathfrak{L}_\alpha \subseteq \langle\langle \bar{A} \rangle\rangle$ und $\mathfrak{L}_\beta \subseteq \langle\langle \bar{B} \rangle\rangle$ mit den Bezeichnungen aus (1.2), (1.3) und (1.29). Ferner legen wir $s_\alpha, s_\beta \geqslant 1$ fest durch

$$s_\alpha := \max_{i \in \mathscr{I}} \max(|\alpha^{(i)}|, |\alpha^{(i)}|^{-1}), \qquad s_\beta := \max_{i \in \mathscr{I}} \max(|\beta^{(i)}|, |\beta^{(i)}|^{-1}).$$

LEMMA 1.22. *Definiere* $S_0 > 1$ *durch*

$$S_0 := \max_{i \in \mathscr{I}} \max\left(\bar{A}, \frac{1 + |\beta^{(i)}|\ \bar{B}}{|\alpha^{(i)}|}\right). \tag{1.42}$$

Für jedes $j \in \mathscr{I}$ *setze mittels* (1.30) *ferner*

$$V_j := U_j\left(\beta, \frac{|\alpha^{(j)}|}{S_0}, s_\beta \bar{B}\right).$$

Mit $V := V_1 \cup \ldots \cup V_{r_1+r_2}$ *gilt dann*

$$\mathfrak{L} \subseteq \{(a, b) \in \mathfrak{L} \mid a \in \langle\langle S_0 \rangle\rangle\} \cup \{(a, b) \in \mathfrak{L} \mid b \in V\}.$$

Beweis. Sei $(a, b) \in \mathfrak{L}$ beliebig. Es gelte ohne Einschränkung $a \notin \langle\langle S_0 \rangle\rangle$, also $b \in \mathfrak{L}_\beta$ wegen $\mathfrak{L}_\alpha \subseteq \langle\langle S_0 \rangle\rangle$. Aus der Definition von S_0 folgt

$$|a^{(i)}| = \left|\frac{1 - (\beta b)^{(i)}}{\alpha^{(i)}}\right| \leqslant S_0 (i \in \mathscr{I}).$$

Aufgrund von $a \notin \langle\langle S_0 \rangle\rangle$ existiert demnach ein $j \in \mathscr{I}$ mit $|a^{(j)}| \leqslant 1/S_0$. Also

$$|(\beta b)^{(j)} - 1| = |(\alpha a)^{(j)}| < \frac{|\alpha^{(j)}|}{S_0}, \tag{1.43}$$

und damit $b \in V_j$. ∎

LEMMA 1.23. *Es seien* s, S *gegeben mit* $s_\alpha < s < S$, *und es sei* $U(\rho, \delta, s) \subseteq \mathrm{U}_{\mathscr{K}}$ *definiert als*

$$U(\rho, \delta, s) := \bigcup_{j \in \mathscr{I}} U_j(\rho, \delta, s).$$

Setze ferner

$$T_\pm := U\left(\alpha^{\pm 1}, \frac{1}{1 + s_\alpha S}, s_\alpha S\right),$$

$$T' := U\left(\beta, \frac{s_\alpha}{s}, 1 + s_\alpha S\right), \qquad T'' := U\left(-\frac{\beta}{\alpha}, \frac{s_\alpha}{s}, 1 + s_\alpha S\right).$$

Dann gilt für alle $(a, b) \in \mathfrak{L}$ *mit* $a \in \langle\langle S \rangle\rangle$ *stets* $a \in \langle\langle s \rangle\rangle$ *oder eine der vier Bedingungen* $a \in T_+$, $a^{-1} \in T_-$, $b \in T'$, $b/a \in T''$.

Beweis. Sei $(a, b) \in \mathfrak{L}$ beliebig mit $a \in \langle\langle S \rangle\rangle$. Es gelte ohne Einschränkung $a \notin \langle\langle s \rangle\rangle$ sowie $a \notin T_+$ und $1/a \notin T_-$. Für jedes $i \in \mathscr{I}$ gelten dann die Abschätzungen

$$|(\beta b)^{(i)}| = |(\alpha a)^{(i)} - 1| \geqslant \frac{1}{1 + s_\alpha S}, \tag{1.44}$$

$$\left|\frac{(\beta b)^{(i)}}{(\alpha a)^{(i)}}\right| = \left|\frac{1}{(\alpha a)^{(i)}} - 1\right| \geqslant \frac{1}{1 + s_\alpha S}. \tag{1.45}$$

Ist $|a^{(j)}| < 1/s$ für ein $j \in \mathscr{I}$, so folgt

$$|(\beta b)^{(j)} - 1| = |(\alpha a)^{(j)}| < \frac{s_\alpha}{s}, \tag{1.46}$$

und $a \in \langle\langle S \rangle\rangle$ impliziert

$$|(\beta b)^{(i)}| = |(\alpha a)^{(i)} - 1| \leqslant 1 + s_\alpha S \qquad (i \in \mathscr{I}). \tag{1.47}$$

Die Kombination von (1.44), (1.46) und (1.47) liefert dann $b \in T'$.

Ist $|a^{(j)}| > s$ für ein $j \in \mathscr{I}$, so gilt

$$\left|-\frac{(\beta b)^{(j)}}{(\alpha a)^{(j)}} - 1\right| = \left|\frac{-1}{(\alpha a)^{(j)}}\right| < \frac{s_\alpha}{s}, \tag{1.48}$$

und aus

$$\left|-\frac{(\beta b)^{(i)}}{(\alpha a)^{(i)}}\right| = \left|\frac{1}{(\alpha a)^{(i)}} - 1\right| \leqslant 1 + s_\alpha S \qquad (i \in \mathscr{I})$$

folgt zusammen mit (1.45) und (1.48) dann $b/a \in T''$. ∎

Analog zur Bestimmung von $\mathrm{X}_{\mathscr{K}}$ bei der Berechnung von Ausnahmeeinheiten geben wir uns jetzt zunächst $m \in \mathbb{N}_0$ und $S_1 > ... > S_m$ vor, wobei hier zusätzlich $S_1 < S_0$ mit S_0 aus 1.22 und $S_m > s_\alpha$ gelte. Wir werden schrittweise endliche Mengen $A_0, ..., A_m \subseteq \mathrm{U}_{\mathscr{K}}$ konstruieren, so daß für jedes $k \in \{1, ..., m\}$ die Implikation

$$(a, b) \in \mathfrak{L} \Rightarrow a \in A_k \vee a \in \langle\langle S_k \rangle\rangle, \tag{1.49}$$

erfüllt ist.

S_0 hatten wir bereits in Lemma 1.22 festgelegt. Wählen wir A_0 als

$$A_0 := \left\{ \frac{1-\beta\varepsilon}{\alpha} \in \mathrm{U}_{\mathscr{K}} \mid \varepsilon \in V \right\}.$$

mit V wie in 1.22, so entspricht (1.49) gerade der Aussage von Lemma 1.22.

Ist für $k \in \{0, ..., m-1\}$ die Menge A_k bereits bekannt, so bestimmen wir T_+, T_-, T', T'' aus 1.23, wobei dort $s = S_{k+1}$ und $S = S_k$, und setzen

$$\begin{aligned} A_{k+1} := A_k &\cup \left\{ \varepsilon \in \mathrm{U}_{\mathscr{K}} \mid \left(\varepsilon \in T_+ \vee \frac{1}{\varepsilon} \in T_- \right) \vee \frac{1-\alpha\varepsilon}{\beta} \in \mathrm{U}_{\mathscr{K}} \right\} \\ &\cup \left(\frac{1-\beta\varepsilon}{\alpha} \in \mathrm{U}_{\mathscr{K}} \mid \varepsilon \in T' \right) \\ &\cup \left\{ \frac{1}{\alpha+\beta\varepsilon} \in \mathrm{U}_{\mathscr{K}} \mid \varepsilon \in T'' \right\}. \end{aligned} \tag{1.50}$$

Die Implikation (1.49) gilt dann aufgrund von 1.23.

Da der sich aus diesem Vorgehen ergebende Algorithmus in seinem Aufbau mit Algorithmus 1.16 übereinstimmt, verzichten wir hier auf seine Wiedergabe. Die Komplexitätsbetrachtung, mit der die Wahl von m und $S_1, ..., S_m$ vorgenommen wird, ist im allgemeinen Fall etwas unübersichtlicher. Vereinfachend kann man allerdings annehmen, daß die Bestimmung der Mengen T_+ und T_- in 1.23 für die Komplexität von untergeordneter Bedeutung ist, da nämlich das Volumen der hier auszuzählenden Mengen klein ist im Vergleich zu dem der Mengen, welche bei der Bestimmung von T' und T'' ausgezählt werden müssen. Unter dieser Annahme ergibt sich bei der Komplexitätsbetrachtung für das Vorgehen im allgemeinen Fall ein von der Struktur her zu (1.39) identischer Ausdruck. Dementsprechend kann bei der Wahl von m und $S_1, ..., S_m$ wie im Spezialfall $\alpha = 1 = \beta$ verfahren werden.

Bemerkung 1.24. Sei $d \in \mathbb{N}$ mit $d\alpha, d\beta \in \mathfrak{o}_{\mathscr{K}}$. Ein einfaches Kriterium, mit dem man oftmals sehr schnell feststellen kann, daß die Einheitengleichung (1.1) keine Lösung besitzt, besteht darin, zu zeigen, daß d nicht in $\alpha\mathfrak{o}_{\mathscr{K}} + \beta\mathfrak{o}_{\mathscr{K}}$ liegt.

2. INDEXFORMGLEICHUNGEN

Für ein beliebiges $I \in \mathbb{N}$ besitzt die Menge $\{\alpha \in \mathfrak{o}_{\mathscr{K}} \mid (\mathfrak{o}_{\mathscr{K}} : \mathbb{Z}[\alpha]) = I\}$ nach einem Resultat von Győry [13] ein endliches Vertretersystem $\mathfrak{I}_{\mathscr{K}}(I)$

bzgl. $\mathbb{Z}$-Äquivalenz, wobei zwei ganze algebraische Zahlen $\alpha, \beta \in \mathfrak{o}_{\mathscr{K}}$ $\mathbb{Z}$-äquivalent heißen, sofern $\alpha \pm \beta \in \mathbb{Z}$. Die Berechnung von $\mathfrak{I}_{\mathscr{K}}(I)$ bezeichnet man als das Lösen einer Indexformgleichung. Diese Bezeichnung rührt daher, weil zu einer Ganzheitsbasis $\omega_1 = 1, \omega_2, ..., \omega_n$ von $\mathfrak{o}_{\mathscr{K}}$ eine Form $I_{\mathscr{K}}(t_2, ..., t_n) \in \mathbb{Z}[t_2, ..., t_n]$ mit der Eigenschaft existiert, daß für alle $\alpha = x_1\omega_1 + \cdots + x_n\omega_n \in \mathfrak{o}_{\mathscr{K}}$ mit $(\mathfrak{o}_{\mathscr{K}} : \mathbb{Z}[\alpha]) < \infty$ jeweils

$$(\mathfrak{o}_{\mathscr{K}} : \mathbb{Z}[\alpha]) = \pm I_{\mathscr{K}}(x_2, ..., x_n). \tag{2.51}$$

gilt. Die Form $I_{\mathscr{K}}$ nennt man Indexform von $\mathscr{K}$ bzgl. $\omega_1, ..., \omega_n$.

Wir werden in diesem Abschnitt unser Verfahren für Einheitengleichungen auf das Lösen von Indexformgleichungen anwenden. Dazu benutzen wir hauptsächlich die klassische Methode, mit welcher Győry die Endlichkeit von $\mathfrak{I}_{\mathscr{K}}(I)$ dadurch bewies, daß er die effektive Berechnung von $\mathfrak{I}_{\mathscr{K}}(I)$ auf das Lösen endlich vieler Einheitengleichungen in der galoisschen Hülle von $\mathscr{K}$ zurückführte. Mit unserer Ausarbeitung von Győrys Methode zu einem Algorithmus, welche sich teilweise auf zwei Arbeiten von Smart [23, 24] stützt, lösten wir erstmals Indexformgleichungen in Zahlkörpern von Grad, 8, 10 und 12. Daneben verwendeten wir eine Idee von Niklasch [19], um in den Kreisteilungskörpern $\mathbb{Q}(\zeta_{17})$, $\mathbb{Q}(\zeta_{19})$ un $\mathbb{Q}(\zeta_{23})$ alle Potenzganzheitsbasen zu berechnen.

Die Anwendbarkeit von Győrys Methode ist in der Praxis eingeschränkt durch die Notwendigkeit, Rechnungen in der galoisschen Hülle von $\mathscr{K}$ durchführen zu müssen. Alternative Verfahren zum Lösen von Indexformgleichungen, welche nicht der galoisschen Hülle bedürfen, existieren bislang nur für Zahlkörper vom Grad $\leqslant 4$. Für kubische Zahlkörper zeigten Gaál und Schulte [11], daß die Bestimmung von $\mathfrak{I}_{\mathscr{K}}(I)$ äquivalent ist zum Lösen einer kubischen Thue-Gleichung, für quartische Zahlkörper entwickelten Gaál, Pethő un Pohst [8, 9] ein Verfahren, bei dem die Berechnung von $\mathfrak{I}_{\mathscr{K}}(I)$ im wesentlichen auf das Lösen eines Systems ternärer quadratischer Formen zurückgeführt wird. Darüber hinaus existieren Verfahren von Gaál [6, 7] sowie von Gaál und Pohst [10] für spezielle Körper sechsten Grades.

Zur weiteren Formulierung legen wir einige Notationen fest. Wie üblich in dieser Arbeit sei $\mathscr{K}$ gegeben als $\mathscr{K} = \mathbb{Q}(\theta)$ mit einer ganzen algebraischen Zahl θ. Wir wählen $d \in \mathbb{N}$ mit $d\mathfrak{o}_{\mathscr{K}} \subseteq \mathbb{Z}[\theta]$. Ferner bezeichnen wir die galoissche Hülle von $\mathscr{K}$ mit $\mathscr{L}$ und setzen $m := [\mathscr{L} : \mathbb{Q}]$. Für die Galoisgruppe von $\mathscr{L}/\mathbb{Q}$ schreiben wir G. Da das Lösen einer Indexformgleichung für $n = [\mathscr{K} : \mathbb{Q}] \leqslant 2$ trivial ist, sei ohne Einschränkung $n \geqslant 3$.

Wir setzen

$$N := \{1, ..., n\},$$
$$N_2 := \{\{i, j\} \mid 1 \leqslant i < j \leqslant n\},$$
$$N_3 := \{\{i, j, k\} \mid 1 \leqslant i < j < k \leqslant n\}.$$

Es seien $\pi_1, ..., \pi_k \in N_3$ so gewählt, daß zu jedem $\tau \in N_2$ ein π_j $(1 \leqslant j \leqslant k)$ existiere mit $\tau \subseteq \pi_j$. Für jedes π_i $(2 \leqslant i \leqslant k)$ gelte darüber hinaus

$$\exists j \in \{1, ..., i-1\} \qquad \text{mit} \quad \pi_i \cap \pi_j \in N_2. \tag{2.52}$$

Die Galoisgruppe G operiere auf den Mengen N, N_2 und N_3 vermöge

$$G \times N \to N: (\sigma, i) \mapsto \sigma \cdot i := i', \qquad \text{wo} \quad \sigma(\theta^{(i)}) = \theta^{(i')},$$
$$G \times N_2 \to N_2: (\sigma, \{i, j\}) \mapsto \sigma \cdot \{i, j\} := \{\sigma \cdot i, \sigma \cdot j\},$$
$$G \times N_3 \to N_3: (\sigma, \{i, j, k\}) \mapsto \sigma \cdot \{i, j, k\} := \{\sigma \cdot i, \sigma \cdot j, \sigma \cdot k\}.$$

Es sei S_2 bzw. S_3 ein Vertretersystem der G-Bahnen von N_2 bzw. N_3. Zu $\tau \in N_2$ sei $\mathscr{F}_\tau$ der Fixkörper des Stabilisators von τ in G. Schließlich setzen wir $\mathscr{K}_\tau := \mathbb{Q}(\theta^{(i)}, \theta^{(j)})$ für $\tau = \{i, j\} \in N_2$ und weiter $\mathscr{K}_\pi := \mathbb{Q}(\theta^{(i)}, \theta^{(j)}, \theta^{(k)})$ für $\pi = \{i, j, k\} \in N_3$.

Für jedes $\alpha \in \mathfrak{I}_{\mathscr{K}}(I)$ und jedes $\tau = \{i, j\} \in N_2$ ist nach Wahl von d

$$\alpha_\tau := \frac{d(\alpha^{(i)} - \alpha^{(j)})}{\theta^{(i)} - \theta^{(j)}} \tag{2.53}$$

eine ganze algebraische Zahl aus $\mathscr{F}_\tau$. Es gilt

$$d^{n(n-1)} I^2 \operatorname{disc}_{\mathscr{K}} = d^{n(n-1)} \prod_{\{i, j\} \in N_2} (\alpha^{(i)} - \alpha^{(j)})^2$$
$$= \prod_{\{i, j\} \in N_2} (\theta^{(i)} - \theta^{(j)})^2 \alpha_{ij}^2,$$

wobei wir im rechten Produkt α_{ij} anstatt $\alpha_{\{i, j\}}$ geschrieben haben—eine schreibtechnische Vereinfachung, die wir im folgenden bei Indizierungen mit Elementen aus N_2 und N_3 beibehalten. Setzen wir

$$I' := I^2 \frac{d^{n(n-1)} \operatorname{disc}_{\mathscr{K}}}{\operatorname{disc} \mathbb{Z}[\theta]} \in \mathbb{N},$$

so erhalten wir für jedes $\alpha \in \mathfrak{I}_{\mathscr{K}}(I)$ die Gleichung

$$I' = \prod_{\tau \in N_2} \prod_{\sigma \in G_\tau} \sigma(\alpha_{\tau_j})^2, \tag{2.54}$$

wo G_τ ein Vertretersystem der Nebenklassen σH_τ des Stabilisators H_τ von τ in G bezeichnet.

Die Gleichung (2.54) ist der Ausgangspunkt für das im folgenden dargestellte Verfahren zur Lösung der Indexformgleichung, welches wir in vier Schritte gliedern.

2.1. *Erster Schritt*

Im ersten Schritt zur Berechnung von $\mathfrak{I}_{\mathscr{K}}(I)$ ermitteln wir eine endliche Menge $A \subseteq \prod_{\tau \in S_2} \mathscr{F}_\tau$ derart, daß zu jedem $\alpha \in \mathfrak{I}_{\mathscr{K}}(I)$ ein $a = (a_\tau) \in A$ existiert mit

$$\alpha_\tau \in a_\tau \mathfrak{U}_{\mathscr{F}_\tau} \qquad (\tau \in S_2). \tag{2.55}$$

Für $I' = 1$, also $I = d = 1$, leistet offensichtlich $A = \{(1, ..., 1)\}$ das Gewünschte. Im Fall $I' \neq 1$ erhält man A aus den Primfaktorisierungen

$$I' \mathfrak{o}_{\mathscr{L}} = \prod_{j=1}^{r} \mathfrak{p}_j^{e_j}, \qquad \alpha_\tau \mathfrak{o}_{\mathscr{L}} = \prod_{\mu=1}^{r} \mathfrak{p}_\mu^{e_{\mu\tau}}, \qquad \prod_{\sigma \in G_\tau} \sigma(\mathfrak{p}_\mu)^2 = \prod_{j=1}^{r} \mathfrak{p}_j^{\lambda_{j\mu r}},$$

die über das lineare Gleichungssystem

$$e_j = \sum_{\mu=1}^{r} \sum_{\tau \in S_2} \lambda_{j\mu r} e_{\mu\tau} \qquad (1 \leqslant j \leqslant r) \tag{2.56}$$

verknüpft sind. In

$$\mathfrak{L} := \left\{ (x_{\mu\tau}) \in (\mathbb{N}_0^r)_{\tau \in S_2} \mid e_j = \sum_{\mu,\, \tau} \lambda_{j\mu\tau} x_{\mu\tau} \right\}$$

werden die Exponentensysteme $(x_{\mu\tau})$ bestimmt, zu denen ein $(a_\tau) \in \prod_{\tau \in S_2} \mathscr{F}_\tau$ existiert mit

$$a_\tau \mathfrak{o}_{\mathscr{L}} = \prod_{\mu=1}^{r} \mathfrak{p}_\mu^{x_{\mu\tau}} \qquad (\tau \in S_2). \tag{2.57}$$

Im Falle der Existenz solcher Hauptideale wird ein Erzeugersystem (a_τ) zu A hinzugefügt.

Bemerkung 2.1. Neben der Hauptidealbedingung aus (2.57) wird die Menge der für A brauchbaren Exponentensysteme aus $\mathfrak{L}$ über die folgenden beiden Kriterien eingeschränkt:

(1) Sei $I=1$, und sei ferner $\alpha \in \mathfrak{I}_{\mathscr{K}}(I)$ beliebig. Dann gilt $\mathbb{Z}[\theta] \subseteq \mathbb{Z}[\alpha]$. Für jedes $\tau=\{i, j\} \in N_2$ teilt also $\alpha^{(i)}-\alpha^{(j)}$ die Differenz $\theta^{(i)}-\theta^{(j)}$ in $\mathfrak{o}_{\mathscr{F}_\tau}$. Somit muß für ein $(a_\tau) \in A$ jedes a_τ ein Teiler von d in $\mathfrak{o}_{\mathscr{F}_\tau}$ sein. Ist $\mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_r^{d_r}$ die Primidealzerlegung von d in $\mathfrak{o}_{\mathscr{L}}$, so gilt für jedes $(x_{\mu\tau}) \in \mathfrak{L}$, welches mit einer Lösung aus $\mathfrak{I}_{\mathscr{K}}(I)$ korrespondiert, also $x_{\mu\tau} \leqslant d_\mu$.

(2) Sei $\mathscr{K}$ normal mit abelscher Galoisgruppe G, und seien ferner $\alpha \in \mathfrak{I}_{\mathscr{K}}(I)$ sowie $\{i, j\} \in N_2$ beliebig vorgegeben. Für jedes $\sigma \in G$ ist dann wegen

$$\sigma(d(\alpha^{(i)}-\alpha^{(j)}))=d((\sigma(\alpha))^{(i)}-(\sigma(\alpha))^{(j)})$$

die Differenz $\theta^{(i)}-\theta^{(j)}$ ein Teiler von $\sigma(d(\alpha^{(i)}-\alpha^{(j)}))$ in $\mathfrak{o}_{\mathscr{K}}$. Für ein $(a_\tau) \in A$ muß also

$$\frac{\sigma(\theta^{(i)}-\theta^{(j)})\,\sigma(a_\tau)}{\theta^{(i)}-\theta^{(j)}} \qquad (\tau \in S_2,\ \{i, j\}=\tau)$$

stets eine ganze algebraische Zahl aus $\mathfrak{o}_{\mathscr{K}}$ sein.

Beispiel 2.2. Sei $\mathscr{K}=\mathbb{Q}(\theta)$, wo θ Nullstelle von $t^5-10t^3+5t^2+10t+1$. Dann hat $\mathscr{K}$ die Klassenzahl 1 und ist normal mit Galoisgruppe $C(5)$, so daß N_2 aus den beiden G-Bahnen von $S_2=\{(1, 2), (1, 3)\}$ besteht. Eine Ganzheitsbasis von $\mathfrak{o}_{\mathscr{K}}$ ist gegeben durch

$$\omega_1=1, \quad \omega_2=\theta, \quad \omega_3=\theta^2, \quad \omega_4=\theta^3, \quad \omega_5=\frac{2+2\theta+6\theta^2+3\theta^3+\theta^4}{7}.$$

Wegen $(\mathfrak{o}_{\mathscr{K}} : \mathbb{Z}[\theta])=7$ können wir $d=7$ wählen.

Wir wollen $i_{\mathscr{K}} \in \mathbb{N}$ minimal mit $\mathfrak{I}_{\mathscr{K}}(i_{\mathscr{K}}) \neq \varnothing$ bestimmen und das Vertretersystem $\mathfrak{I}_{\mathscr{K}}(i_{\mathscr{K}})$ explizit berechnen. Da $\mathscr{K}$ nicht der maximale reelle Teilkörper eines Kreisteilungskörpers ist, gilt $\mathfrak{I}_{\mathscr{K}}(1)=\varnothing$ nach einem Resultat von M. N. Gras [12]. Wegen $\theta \in \mathfrak{I}_{\mathscr{K}}(7)$ müssen wir also herausfinden, für welches minimale $I \in \{2, 3, 4, 5, 6, 7\}$ die Menge $\mathfrak{I}_{\mathscr{K}}(I)$ nicht leer ist. Dazu geben wir zunächst die Zerlegungen von 2, 3, 5, 7 in paarweise verschiedene Primideale aus $\mathfrak{o}_{\mathscr{K}}$ an:

$$2\mathfrak{o}_{\mathscr{K}}=\mathfrak{p}_1, \qquad 3\mathfrak{o}_{\mathscr{K}}=\mathfrak{p}_2, \qquad 5\mathfrak{o}_{\mathscr{K}}=\mathfrak{p}_3^5, \qquad 7\mathfrak{o}_{\mathscr{K}}=\mathfrak{p}_4\mathfrak{p}_5\mathfrak{p}_6\mathfrak{p}_7\mathfrak{p}_8.$$

Es ist insbesondere

$$\frac{d^{n(n-1)}\,\mathrm{disc}_{\mathscr{K}}}{\mathrm{disc}\,\mathbb{Z}[\theta]}\,\mathfrak{o}_{\mathscr{K}} = 7^{18}\mathfrak{o}_{\mathscr{K}} = \mathfrak{p}_4^{18}\mathfrak{p}_5^{18}\mathfrak{p}_6^{18}\mathfrak{p}_7^{18}\mathfrak{p}_8^{18}.$$

Im folgenden bezeichne Π die 5×5-Matrix, deren sämtliche Einträge 2 sind, und $\underline{z}$ die Spalte mit fünf Einträgen z.

1. Fall $I=2,3$. Es ist $\mathfrak{I}_{\mathscr{K}}(2)=\varnothing=\mathscr{I}_{\mathscr{K}}(3)$, da das lineare Gleichungssystem

$$\begin{pmatrix}2\\ \underline{18}\end{pmatrix}=\begin{pmatrix}10 & \underline{0}^t & 10 & \underline{0}^t\\ \underline{0} & \Pi & \underline{0} & \Pi\end{pmatrix}\cdot x$$

aus (2.56) keine Lösung in $\mathbb{N}_0^{12}$ besitzt.

2. Fall $I=4,6$. Es ist $\mathfrak{I}_{\mathscr{K}}(4)=\varnothing=\mathfrak{I}_{\mathscr{K}}(6)$, wie man leicht anhand des Gleichungssystems aus dem Fall $\mathrm{I}=2,3$ folgert.

3. Fall $I=5$. Wir erhalten das lineare Gleichungssystem

$$\begin{pmatrix}10\\ \underline{18}\end{pmatrix}=\begin{pmatrix}10 & \underline{0}^t & 10 & \underline{0}^t\\ \underline{0} & \Pi & \underline{0} & \Pi\end{pmatrix}\cdot x$$

mit 97240 Lösungen in $\mathbb{N}_0^{12}$. Von diesen können wir 93236 viele vermöge des zweiten Kriteriums aus 2.1 aussortieren. Für $I=5$ enthält A also 4004 Elemente.

4. Fall $I=7$. Wir erhalten das lineare Gleichungssystem

$$(\underline{20})=(\Pi\quad\Pi)\cdot x$$

mit 92378 Lösungen in $\mathbb{N}_0^{10}$. Von diesen können wir 87373 viele vermöge des zweiten Kriteriums aus 2.1 aussortieren. Für $I=7$ enthält A also 5005 Elemente.

Wir werden dieses Beispiel später fortsetzen.

Für den Rest dieses Abschnitts sei $a=(a_\tau)\in A$ beliebig, aber fest vorgegeben. Setzen wir

$$\mathfrak{I}_{\mathscr{K}}(I,a):=\{\alpha\in\mathfrak{I}_{\mathscr{K}}(a)\mid \alpha \text{ ist äquivalent zu } a \text{ vermöge } (2.55)\}$$

und weiter $a_{\sigma\cdot\tau}:=\sigma(a_\tau)$ $(\sigma\in G,\tau\in S_2)$, so gilt für ein $\alpha\in\mathfrak{I}_{\mathscr{K}}(I,a)$ jeweils

$$\alpha_\tau\in a_\tau \mathrm{U}_{\mathscr{F}_\tau}\qquad\forall\tau\in N_2. \tag{2.58}$$

2.2. *Zweiter Schritt*

Wir verwenden jetzt die eingangs bei (2.52) gewählten $\pi_1, ..., \pi_k \in N_3$. Für jedes dieser π_v berechnen wir eine endliche Menge $U_v(a) \subseteq \prod_{\tau \in N_2,\, \tau \subseteq \pi_v} U_{\mathscr{F}_\tau}$ derart, daß zu jedem $\alpha \in \mathfrak{I}_{\mathscr{K}}(I, a)$ ein Tripel $(\varepsilon_{v\tau}) \in U_v(a)$ und eine Einheit $\eta_v \in U_{\mathscr{L}}$ existieren mit

$$\alpha_\tau = a_\tau \varepsilon_{v\tau} \eta_v \qquad (\tau \in N_2,\, \tau \subseteq \pi_v). \tag{2.59}$$

Dazu benützen wir die Einschränkungen, denen die Faktoren $\varepsilon_\tau \in \mathrm{U}_{\mathscr{F}_\tau}$ mit $\alpha_\tau = a_\tau \varepsilon_\tau$ in (2.58) unterliegen: Für $\pi_v = \{i, j, k\}$ folgt aus

$$\alpha^{(i)} - \alpha^{(j)} + \alpha^{(j)} - \alpha^{(k)} = \alpha^{(i)} - \alpha^{(k)}$$

die Einheitengleichung

$$\frac{(\theta^{(i)} - \theta^{(j)})\, a_{ij}}{(\theta^{(i)} - \theta^{(k)})\, a_{ik}} \frac{\varepsilon_{ij}}{\varepsilon_{ik}} + \frac{(\theta^{(j)} - \theta^{(k)})\, a_{jk}}{(\theta^{(i)} - \theta^{(k)})\, a_{ik}} \frac{\varepsilon_{jk}}{\varepsilon_{ik}} = 1, \tag{2.60}$$

deren Lösungsmenge uns $U_v(a)$ unmittelbar liefert.

2.3. *Dritter Schritt*

Anhand der Mengen $U_1(a), ..., U_k(a)$ bestimmen wir als nächstes eine endliche Menge $U(a) \subseteq \prod_{\tau \in N_2} \mathrm{U}_{\mathscr{F}_\tau}$ mit der Eigenschaft, daß zu jedem $\alpha \in I_{\mathscr{K}}(I, a)$ ein $(u_\tau) \in U(a)$ und eine Einheit $\varepsilon \in \mathrm{U}_{\mathscr{L}}$ existieren mit

$$\alpha_\tau = a_\tau u_\tau \varepsilon \qquad (\tau \in N_2). \tag{2.61}$$

Sei dazu $\alpha \in I_{\mathscr{K}}(I, a)$ beliebig, aber fest vorgegeben. Für jedes $v \in \{1, ..., k\}$ sei $(\varepsilon_{v\tau}) \in U_v(a)$ das zu α passende Tripel mit der Eigenschaft aus (2.59). Setzen wir $u_\tau = \varepsilon_{1\tau}$ für jedes $\tau \in N_2$ mit $\tau \subseteq \pi_1$, so ist (2.61) für eben diese τ erfüllt. Sei nun $v \in \{2, ..., k\}$, und für alle $\tau \in N_2$, die in einem π_i $(1 \leqslant i < v)$ enthalten sind, seien bereits Einheiten u_τ bestimmt, welche (2.61) erfüllen. Ist dann $\{\tau \in N_2 \mid \tau \subseteq \pi_v\} = \{\tau, \tau', \tau''\}$, so können wir wegen (2.52) ohne Einschränkung annehmen, daß ein $i \in \{1, ..., v-1\}$ existiert mit $\tau \subseteq \pi_i$. Mit $\varepsilon \in \mathrm{U}_{\mathscr{L}}$ wie in (2.61) folgt dann $\varepsilon_{v\tau} \eta_v = u_\tau \varepsilon$. Setzen wir also

$$u_{\tau'} := \varepsilon_{v\tau'} \frac{u_\tau}{\varepsilon_{v\tau}}, \qquad u_{\tau''} := \varepsilon_{v\tau''} \frac{u_\tau}{\varepsilon_{v\tau}}, \tag{2.62}$$

so ist (2.61) auch für τ', τ'' erfüllt.

2.4. *Vierter Schritt*

Abschließend kann jetzt $I_{\mathscr{K}}(I, a)$ aus $U(a)$ bestimmt werden. Sei $(u_\tau) \in U(a)$ gegeben, welches vermöge (2.61) mit einem $\alpha \in I_{\mathscr{K}}(I, a)$ korrespondiert. Aus (2.54) erhalten wir die Gleichung

$$I' = \varepsilon^{n(n-1)} \prod_{\tau \in N_2} a_\tau^2 u_\tau^2,$$

mit der ε bis aus eine Einheitswurzel eindeutig bestimmt ist. Für alle $\{i, j\} \in N_2$ kennen wir damit die Differenzen $\alpha^{(i)} - \alpha^{(j)}$, anhand derer sich α modulo $\mathbb{Z}$-Äquivalenz wie folgt berechnen läßt: Es sei $\omega_1 = 1, ..., \omega_n$ bzw. $v_1 = 1, ..., v_m$ eine Ganzheitsbasis von $\mathfrak{o}_{\mathscr{K}}$ bzw. $\mathfrak{o}_{\mathscr{L}}$. Zu den Zeilen $\omega = (\omega_1, ..., \omega_n)$ und $v = (v_1, ..., v_m)$ existieren Matrizen $T \in \mathbb{Z}^{m \times n}$ und $T_i \in \mathrm{GL}_m(\mathbb{Z})$ $(1 \leqslant i \leqslant m)$ mit $v \cdot T = \omega$ und $\sigma_i v = v \cdot T_i$. Dann liefert das Matrizenprodukt $\alpha = \omega \cdot x$ $(x \in \mathbb{Z}^m)$ die Gleichung

$$\alpha^{(i)} - \alpha^{(j)} = v \cdot \xi_{ij} = v \cdot (T_i - T_j) \cdot T \cdot x \qquad (1 \leqslant i, j \leqslant n).$$

Folglich ist $\xi_{ij} = (T_i - T_j) \cdot x$, woraus sich x und damit auch α ergeben.

Mit dem vierten Schritt ist die Ausarbeitung von Győrys Methode zu einem Algorithmus abgeschlossen. Seine Effizienz kann durch eine einfache, auf Smart [23] zurückgehende Modifikation deutlich gesteigert werden: Existiert zu $\pi_\nu, \pi_\mu \in \{\pi_1, ..., \pi_k\}$ ein $\sigma \in G$ mit $\sigma \cdot \pi_\nu = \pi_\mu$, so genügt es zur Bestimmung von $U_\nu(a)$ und $U_\mu(a)$ im zweiten Schritt, die zu π_ν gehörende Einheitengleichung in (2.60) zu lösen. Aus deren Lösungsmenge erhält man allein durch Anwendung von σ die Lösungen der Einheitengleichung zu π_μ.

Beispiel 2.3 (Fortsetzung von 2.2). Entsprechend den schon erzielten Ergebnissen verbleibt die Bestimmung von $\mathfrak{I}_{\mathscr{K}}(I)$ für $I \in \{5, 7\}$. Ist $I = 5$, so sind 4004 Einheitengleichungen im zweiten Schritt zu lösen. Bei den meisten dieser Gleichungen kann man sehr schnell anhand des Kriteriums aus 1.24 feststellen, daß sie keine Lösungen besitzen. Lediglich für eine Einheitengleichung müssen alle drei Schritte des Verfahrens aus dem ersten Abschnitt durchgeführt werden. Da aus den Lösungen dieser Gleichungen kein $\alpha \in \mathfrak{o}_{\mathscr{K}}$ mit $(\mathfrak{o}_{\mathscr{K}} : \mathbb{Z}[\alpha]) = 5$ konstruiert werden kann, gilt $\mathfrak{I}_{\mathscr{K}}(5) = \varnothing$. Die für dieses Ergebnis notwendige Rechenzeit betrug insgesamt 743s. Davon entfallen 139 Sekunden auf den zweiten Schritt, also auf das Lösen der Einheitengleichung, weniger als eine Sekunde auf den dritten und vierten Schritt und der große Rest auf den ersten Schritt, d.h. die Bestimmung vom A.

Es ist jetzt bereits $i_{\mathscr{K}} = 7$ bekannt. Wie im Fall $I = 5$ kann für den Großteil der 5005 Einheitengleichungen, welche zur expliziten Berechnung von $\mathfrak{I}_{\mathscr{K}}(7)$ zu betrachten sind, leicht entschieden werden, daß sie keine Lösungen besitzen. Aus den restlichen zehn Einheitengleichungen, welche mit den Methoden des ersten Abschnitts gelöst werden müssen, ergibt sich für $\mathfrak{I}_{\mathscr{K}}(7)$ das folgende 25-elementige Vertretersystem:

$$\begin{aligned}\mathfrak{I}_{\mathscr{K}}(7) = \{&\omega_4+\omega_5, 4\omega_3-3\omega_4-4\omega_5, \omega_2, \omega_2+\omega_3-\omega_4-\omega_5,\\ &2\omega_2-3\omega_3+2\omega_4+3\omega_5, 2\omega_2+\omega_3-\omega_4-\omega_5,\\ &2\omega_2+6\omega_3-5\omega_4-6\omega_5, 3\omega_2-3\omega_3+\omega_4+2\omega_5,\\ &3\omega_2-3\omega_3+2\omega_4+3\omega_5, 3\omega_2-2\omega_3+\omega_4+2\omega_5,\\ &4\omega_2-3\omega_3+\omega_4+2\omega_5, 4\omega_2-2\omega_3+\omega_4+2\omega_5, 5\omega_2-2\omega_3+\omega_5,\\ &5\omega_2-2\omega_3+\omega_4+2\omega_5, 6\omega_2-6\omega_3+3\omega_4+5\omega_5, 6\omega_2-2\omega_3+\omega_5,\\ &7\omega_2-6\omega_3+3\omega_4+5\omega_5, 8\omega_2-5\omega_3+2\omega_4+4\omega_5,\\ &9\omega_2-5\omega_3+2\omega_4+4\omega_5, 10\omega_2-9\omega_3+4\omega_4+7\omega_5,\\ &13\omega_2-7\omega_3+3\omega_4+6\omega_5, 14\omega_2-12\omega_3+7\omega_4+11\omega_5,\\ &15\omega_2-8\omega_3+3\omega_4+6\omega_5, 22\omega_2-13\omega_3+4\omega_4+9\omega_5,\\ &23\omega_2-11\omega_3+3\omega_4+8\omega_5\}.\end{aligned}$$

Die Rechenzeit betrug insgesamt 1442s mit 779s für den zweiten Schritt und etwa einer Sekunde für den dritten und vierten Schritt.

Eine Inspektion des Resultats zeigt im übrigen, daß $\mathfrak{v}_{\mathscr{K}}$ genau 2 Klassen nichtisomorpher Gleichungsordnungen vom Index 7 besitzt. Die Ordnungen der ersten Klasse besitzen modulo $\mathbb{Z}$-Äquivalenz 2 Potenzbasiserzeuger, während die Ordnungen der zweiten Klasse jeweils über 3 Potenzbasiserzeuger modulo $\mathbb{Z}$-Äquivalenz verfügen.

Neben diesem Beispiel haben wir mit Győrys Methode Indexformgleichungen in Kreisteilungskörpern und ihren maximalen reellen Teilkörpern gelöst. Und zwar bestimmten wir dort jeweils alle Potenzganzheitsbasen modulo $\mathbb{Z}$-Äquivalenz, d.h. genauer, wir berechneten $\mathfrak{I}_{\mathscr{K}_m}(1)$ und $\mathfrak{I}_{\mathscr{K}_m^+}(1)$ für alle $m \in \mathbb{N}$, $m \not\equiv 2 \bmod 4$, mit $[\mathscr{K}_m : \mathbb{Q}] \leqslant 12$, wobei an die im Unter-abschnitt 1.3.2 eingeführte Notation für Kreisteilungskörper erinnert sei.

Der Einsatz von Győrys Methode ist für Kreisteilungskörper höheren Grades sehr aufwendig (siehe etwa $\mathbb{Q}(\zeta_{13})$ in der Tabelle). Die Ursache hierfür liegt sowohl im zweiten Schritt, also dem Lösen der Einheitengleichungen, als auch bei der Kombination der Mengen $U_v(a)$ im dritten Schritte, wobei die Mächtigkeit dieser Mengen mit wachsendem Einheitenrang erfahrungsgemäß stark zunimmt.

Für spezielle Kreisteilungskörper, nämlich dann, wenn m eine Primzahl ist, kann allerdings ein von Niklasch [19, Abschnitt II-4.3] entwickeltes Verfahren eingesetzt werden, welches anhand der Ausnahmeeinheiten alle Potenzganzbasen von $\mathcal{K}_m$ modulo $\mathbb{Z}$-Äquivalenz bestimmt. Der große Vorteil dieses Verfahrens besteht darin, daß sein Aufwand linear ist in der Anzahl der Ausnahmeeinheiten. Allerdings konnte Niklaschs Verfahren in der Vergangenheit nur bis $m \leqslant 7$ praktisch eingesetzt werden, da die Berechnung aller Ausnahmeeinheiten von $\mathcal{K}_m$ für größere Werte von m bislang nicht möglich war.

TABELLE III

m	$[\mathcal{K}_m^+ : \mathbb{Q}]$	$\lvert\mathfrak{I}_{\mathcal{K}_m^+(1)}\rvert$	t	$[\mathcal{K}_m : \mathbb{Q}]$	$\lvert\mathfrak{I}_{K_m}(1)\rvert$	t
1	1	1	—	1	1	—
3	1	1	—	2	1	—
4	1	1	—	2	1	—
5	2	1	—	4	6	0s
7	3	9	3s	6	9	15s
8	2	1	—	4	2	0s
9	3	6	2s	6	9	50s
11	5	25	47s	10	15	2900s
12	2	1	—	4	4	0s
13	6	36	2576s	12	18	34195s
15	4	12	27s	8	16	891s
16	4	6	24s	8	4	303s
20	4	10	23s	8	8	951s
21	6	30	1750s	12	24	32872s
24	4	6	27s	8	8	804s
28	6	15	639s	12	12	31004s
36	6	15	681s	12	12	21066s

Wir haben mit diesem Verfahren anhand der im ersten Abschnitt erzielten Resultate zu Ausnahmeeinheiten in Kreisteilungskörpern alle Potenzganzheitsbasen in $\mathbb{Q}(\zeta_{17})$, $\mathbb{Q}(\zeta_{19})$ und $\mathbb{Q}(\zeta_{23})$ bestimmt. Die Ergebnisse dieser Rechnungen und die der Tabelle III entsprechen einer von Bremner [2] geäußerten Vermutung, welche bislang nur für $p \leqslant 7$ verifiziert war:

Vermutung 2.4 (Bremner). Sei $\zeta_p' \in \mathfrak{o}_{\mathcal{K}_p}$ definiert durch $\zeta_p' := \zeta_p + \cdots + \zeta_p^{(p-1)/2}$. Dann existiert zu jedem $\alpha \in \mathfrak{I}_{\mathcal{K}_p}(1)$ ein Automorphismus σ aus der Galoisgruppe von $\mathcal{K}_p/\mathbb{Q}$, so daß α entweder $\mathbb{Z}$-äquivalent ist zu $\sigma(\zeta_p)$ oder zu $\sigma(\zeta_p')$.

LITERATUR

1. A. Baker und G. Wüstholz, Logarithmic forms and group varieties, *J. Reine Angew. Math.* **442** (1993), 19–62.
2. A. Bremner, On power bases in cyclotomic number fields, *J. Number Theory* **28** (1988), 288–298.
3. M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegener, und K. Wildanger, KANT V4, *J. Symbolic Comput.* **24** (1997), 267–283.
4. J. H. Evertse, Upper bounds for the number of solutions of Diophantine equations, *in* "CWI Tract," Vol. 168, Stichting Mathematisch Centrum, Amsterdam, 1983.
5. U. Fincke und M. Pohst, Improved methods for calculating vectors of short length in a lattice, including a complexity analysis, *Math. Comp.* **44** (1985), 463–471.
6. I. Gaál, Computing all power integral bases in orders of totally real cyclic sextic number fields, *Math. Comp* **65** (1996), 801–822.
7. I. Gaál, Comuting elements of given index in totally complex cyclic sextic fields, *J. Symbolic Comput.* **20** (1995), 61–69.
8. I. Gaál, A. Pethő, und M. Pohst, On the resolution of index form equations in quartic number fields, *J. Symbolic Comput.* **16** (1993), 563–584.
9. I. Gaál, A. Pethő, und M. Pohst, Simultaneous representation of integers by a pair of ternary quadratic forms—With an application to index form equations in quartic number fields, *J. Number Theory* **57** (1996), 90–104.
10. I. Gaál und M. Pohst, On the resolution of index form equations in sextic fields with an imaginary subfield, *J. Symbolic Comput.* **22** (1996), 425–434.
11. I. Gaál und N. Schulte, Computing all power integral bases of cubic fields, *Math. Comp.* **53** (1989), 689–696.
12. M. N. Gras, Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geqslant 5$, *J. Number Theory* **23** (1986), 347–353.
13. K. Győry, Sur l'irréductibilité d'une classe des polynômes, I, *Publ. Math. Debrecen* **18** (1971), 289–307.
14. K. Győry, Sur les polynômes à coefficients entiers et de discriminant donné, II, *Publ. Math. Debrecen* **21** (1974), 125–144.
15. A. K. Lenstra, H. W. Lenstra, Jr., und L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), 515–534.
16. T. Nagell, Sur une propriété des unités d'un corps algébrique, *Ark. Mat.* **5** (1964), 343–356.
17. T. Nagell, Sur les unités dans les corps biquadratiques primitifs du premier rang, *Ark. Mat.* **7** (1968), 359–394.
18. T. Nagell, Sur un type particulier d'unités algébriques, *Ark. Mat.* **8** (1969), 163–184.
19. G. Niklasch, "Einheitengleichungen in kommutativen Ringen," Dissertation, Technische Universität München, München, 1991.
20. G. Niklasch, Family portraits of exceptional units, Manuskript.
21. M. Pohst und H. Zassenhaus, "Algorithmic Algebraic Number Theory," Cambridge Univ. Press, Cambridge, UK, 1989.
22. C. L. Siegel, Über einige Anwendungen diophantischer Approximationen, *Abh. Akad. Wiss. Phys.-Math.* **1** (1929), 209–266.
23. N. P. Smart, The solution of triangularly connected decomposable form equations, *Math. Comp.* **64** (1995), 819–840.
24. N. P. Smart, Discriminant form equations in number fields of degree greater than four, *J. Symbolic Comput.* **21** (1996), 367–374.
25. V. G. Sprindžuk, "Classical Diophantine Equations," Lecture Notes in Mathematics, Vol. 1559, Springer-Verlag, New York/Berlin, 1990.

26. B. M. M. de Weger, Algorithms for diophantine equations, *in* "CWI Tract," Vol. 65, Stichting Mathematisch Centrum, Amsterdam, 1989.
27. K. Wildanger, "Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern mit einer Anwendung auf die Bestimmung aller ganzen Punkte einer Mordellschen Kurve," Dissertation, Technische Universität Berlin, Berlin, 1997.